SIP に係る
既知の脆弱性に関する
調査報告書　改訂第 3 版

IP ネットワーク上のマルチメディアコミュニケーション・システムの
セキュリティ品質向上のために

2010 年 9 月
独立行政法人 情報処理推進機構 セキュリティセンター

登録商標等について
Microsoft、MS、Windows、Windows 2000、Windows NT、Windows XP、Windows ロゴ、Internet Explorer、Outlook、Outlook Express などは、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Sun Microsystems、Sun ロゴ、Java コーヒーカップロゴ、Solaris、Java、JDK などは、米国 Sun Microsystems の米国およびその他の国における登録商標または商標です。
その他、本文章に記載されている会社名、商品名、製品名などは、一般に各社の商標または登録商標です。
本報告書では、™、©、®などを記載しません。

本報告書は、以下の URL からダウンロードできます。

「SIP に係る既知の脆弱性に関する調査報告書」
http://www.ipa.go.jp/security/vuln/vuln_SIP.html

【 1. はじめに 】

改版履歴

版	追加、修正内容
1.0 版(2007 年 12 月)	初版
2.0 版(2009 年 1 月)	SIP/RTP の暗号化に係る脆弱性項目を 3 項目追加(項目 20～22) 項目 20～22 について前書きを追記
	DTLS-SRTP 仕様についての情報を追加修正(項目 8)
	XSS、SQL インジェクションについて追記(項目 18)
	参考情報を追加(項目 6、8、12、14、15、18)
	いくつかの書式スタイルを整理
3.0 版(2010 年 9 月)	RFP 等標準文書を最新の情報に修正
	事象例の追加

目次

1. はじめに....5
2. SIP 仕様解説....11
3. SIP 関連システムの利用形態....23
4. 本報告書記載における前提等....27
5. 脆弱性項目解説....38

■ SIP/SDP に係る脆弱性
項目 1. SIP リクエストの偽装から起こる問題....39
項目 2. SIP レスポンスの偽装から起こる問題....48
項目 3. SIP 認証パスワードの解読....53
項目 4. SIP メッセージボディの改ざんから起こる問題....57
項目 5. 保護されていないトランスポートプロトコルを選択させられる問題....62
項目 6. DoS 攻撃による SIP のサービス妨害....65
項目 7. その他 SIP 拡張リクエストの脆弱性....69

■RTP/RTCP に係る脆弱性
項目 8. RTP メディアの盗聴から起こる問題....73
項目 9. RTP メディアの偽装から起こる問題....79
項目 10. RTCP の偽装から起こる問題....84

■コーデックに係る脆弱性
項目 11. コーデックの脆弱性....92

■実装不良に係る脆弱性
項目 12. 不具合を起こしやすいパケットに対応できない問題....93
項目 13. Call-ID を予測しやすい実装の問題....100
項目 14. 認証機能の不十分な実装の問題....103
項目 15. 送信元 IP アドレスを確認しない実装の問題....108
項目 16. 不適切な IP アドレスを含む SIP メッセージに関する問題....111
項目 17. デバッガ機能へ接続可能な実装の問題....114

■管理機能に係る脆弱性
項目 18. 管理機能に関する問題....117

■ID、構成情報に係る脆弱性
項目 19. 登録 ID と構成情報の収集に関する問題....123

■SIP/RTP の暗号化に係る脆弱性
項目 20. SIP における TLS の不適切な利用から起こる問題....129
項目 21. SRTP の暗号に用いる共通鍵が盗聴される問題....136
項目 22. 暗号化された SRTP が共通鍵なしで解読される問題....141

用語集....145

1. はじめに

本報告書は、SIP に係る既知の脆弱性に関する調査結果をまとめたものである。本章では、まず、本報告書作成の背景、目的、報告書の構成、概要等について記述する。

1.1. 本報告書の背景

SIP（Session Initiation Protocol）はもともと、H.323 や MEGACO などの電話を強く意識したプロトコルに代わって、汎用的な、拡張性の高いセッション開始プロトコルとして IETF（Internet Engineering Task Force）で定義された。その後、チャットやプレゼンス、プッシュツートーク、課金や認証連携などの拡張を経て、携帯電話事業者や固定通信事業者が掲げる、IMS や NGN などの次世代 IP ネットワークの基本的な制御手順として、本格的に利用されるようになった。

すでに、日本国内の IP 電話の発番号数は 2010 年 6 月末時点で 2,300 万以上が発行され（総務省発表）、FTTH ユーザの 56.6%が IP 電話を利用している(「インターネット白書 2007」)。今後、IMS と NGN ではビデオやゲームなども含めたマルチメディア対応のサービスに SIP を活用する方向にあり、現在、テレビ放送の伝送なども含めて、既存の電話網を IP 化するための IMS/NGN 対応の通信機器の導入と一部サービスが進行中である。また、すべてのサービスが IP 上で利用できる「端末の ALL-IP 化」(AIPN: All IP Network)などのインフラ整備も進んでいる。

その一方で、SIP 関連機器への脅威も顕在化している。日本国内では大規模な IP 電話サービスの故障事故があり、米国 SANS によるコンピュータ脆弱性の上位 20 位への VoIP のランクインが報告されている。特に VoIP に関する脆弱性の指摘の中には、VoIP に限らず SIP プロトコルを今後活用するために対策しておかなければならない問題が多い。

2006 年には、数十万台以上のパソコンに感染し、多数のパソコンが同時にあやつられて動作する、ボットネットワークの存在も注目された。2007 年にかけて、家庭用ルータやセットトップボックス、IP 電話機などの組込機器そのもののセキュリティや脆弱性も多数指摘されている。

2008 年には、インターネットと IP 電話網を経由して、一般電話網(PSTN)への無料通信を試みる攻撃の指摘や、第三者による企業内 IP-PBX の不正利用によると見られる多額の国際通話料請求の発生、などの事例がある。また SIP/RTP の制御用に提供されている、管理用の Web インターフェースの SQL インジェクション、XSS/XSRF の脆弱性も指摘されている。

2010 年には、無料通信を試みる攻撃がさらに顕在化し、7 月には警察庁サイバーフォースから、「5060/UDP に対するアクセスの増加について」というレポートが出ている(5060/UDP は SIP で使用されている標準的なポート)。

これらに共通して指摘されているのは、出荷される製品への脆弱性をできるだけ減らすことへの要求である。原理的にソフトウェアの不具合はゼロにすることはできないが、深刻な脆弱性は製品の購入者や利用者に被害を与え、ゆくゆくは製品開発企業や市場自体にダメージを与えることにつながる。

1.2. 本調査の目的

安心・安全な社会基盤を担う製品のセキュリティ品質を向上させるため、製品開発の過程で、製品に入り込む脆弱性を削減することが求められている。そのためには、SIP 関連プロトコルに係る既知の脆弱性について、製品開発者や IP ネットワーク設計者・運用者が理解・検討する必要がある。本資料はこれらの対象者から見て、SIP 関連製品やネットワーク

の企画・設計・開発・運用を行う過程で参考になるよう、SIP 関連プロトコルそのものと、SIP 関連プロトコルを利用した製品に独特な脆弱性情報を収集し、整理している。

1.3. 本報告書の構成

1.3.1. 脆弱性項目の報告

SIP 関連プロトコルの脆弱性に関して、報告や指摘が多く、重要と考えられる情報を 19 項目に分類して報告している。

その内容として、SIP プロトコルに関連する機器や製品の脆弱性の事例や報告として、すでに論文や書籍、ホワイトペーパー、プレゼンテーション資料などとして一般に公開・発表されている情報を収集した。

特に、SIP とは直接関係はない、機器の管理機能やドキュメントについても、SIP 関連機器として現在広く普及しつつある、IP 電話関連機器に多くの脆弱性の指摘があるため、管理に関する問題として項目を設けた。

1.3.2. SIP 関連プロトコル基本仕様、用語集

一般的な SIP 関連プロトコルの概要については、第 2 章「2.1. SIP 関連プロトコル概要」をご覧いただきたい。本報告書を読み進めるにあたって必要となる、基礎的な機能やリクエストとレスポンスのしくみ、典型的な手順の例などを説明している。巻末に用語集も掲載しているのでご利用いただきたい。

脆弱性項目に関する報告書本文の中で、さらに詳細な機能や手順について触れる部分では、その都度、説明を追加している。

なお、複数の脆弱性報告に共通する前提については後述する。

1.4. 脆弱性報告の記述内容

それぞれの脆弱性の報告は、共通して以下の表のような記述を行っている。

表 Ⅰ-1 脆弱性の記述内容

節	段落	内容
概要		その脆弱性の概要。
解説	攻撃手法とその影響	その脆弱性を利用した攻撃の機器の構成、方法、手順と、攻撃の結果として受ける被害や、状態についての説明。
	原因と考察	その脆弱性が指摘された経緯、根本的な原因、対策の候補、注意点など。
対策	運用ガイド	ソフトウェアや機器を利用する、運用者や利用者が、製品の改修が行われる前にとれると考えられる対策案。
	実装ガイド	ソフトウェアや機器の企画・設計者や製品開発者が、製品そのものを改良したり改修するときの対策案。
参考情報		その脆弱性項目の報告に関する技術仕様書、書籍、論文、プレゼンテーション資料などの書名または URL。
CVSS 深刻度評価(参考値)		その脆弱性項目の深刻度を示す参考指標。CVSS v2 の基本評価基準(Base Metrics)で評価した値を掲載した。複数の脆弱性が記述されている場合は、最も深刻度が高い値を代表例として掲載した。

1.5. 脆弱性報告の概要

図 I -1 は本調査報告書において記載を行った脆弱性項目である。

カテゴリ	番号	項目
SIP/SDP	01	SIPリクエストの偽装から起こる問題
	02	SIPレスポンスの偽装から起こる問題
	03	SIP認証パスワードの解読
	04	SIPメッセージボディの改ざんから起こる問題
	05	保護されていないトランスポートプロトコルを選択させられる問題
	06	DoS攻撃によるSIPのサービス妨害
	07	その他SIP拡張リクエストの脆弱性
RTP/RTCP	08	RTPメディアの盗聴から起こる問題
	09	RTPメディアの偽装から起こる問題
	10	RTCPの偽装から起こる問題
コーデック	11	CODECの脆弱性
実装不良	12	不具合を起こしやすいメッセージに対応できない問題
	13	Call-IDを予測しやすい実装の問題
	14	認証機能の不十分な実装の問題
	15	送信元IPアドレスを確認しない実装の問題
	16	複数プロトコルが統合されていない実装の問題
	17	デバッガ機能へ接続可能な実装の問題
管理機能	18	管理機能に関する問題
ID、構成情報	19	登録IDと構成情報の収集に関する問題
SIP/RTP暗号化	20	SIPにおけるTLSの不適切な利用から起こる問題
	21	SRTPの暗号に用いる共通鍵が盗聴される問題
	22	暗号化されたSRTPが共通鍵なしで解読される問題

図 I -1-1 脆弱性項目の一覧

項目 1 から項目 7 は、特に SIP のプロトコルそのものが持っている脆弱性について整理した。SIP の標準仕様自体は暗号化などの通信の保護機能を持たないため、SIP のヘッダやボディを盗聴、改ざんされることがある。項目 1 と項目 2 では、特に SIP プロトコルそのものの脆弱性のうち、原因と対策が共通になるものを SIP のリクエストと SIP のレスポンスとして整理した。

また、項目 4 では SIP のデフォルトの認証手順であるダイジェスト認証が盗聴されると、パスワードを解読される脆弱性を整理した。項目 5 では、こうした問題への対策として使われる TLS 暗号プロトコルが、選択できないよう妨害する手法について整理した。

SIP には、リクエストの種別を示す、SIP メソッドが 14 種類以上、定義、提案されているが、本報告書では特に SIP で中心的に利用されている REGISTER, INVITE などの SIP メソッドについて詳細に記述し、その他の後発の SIP メソッドについては、項目 7 その他 SIP 拡張リクエストの脆弱性として整理した。

項目 8 から項目 10 は、音声やビデオなどのメディアを転送・制御する、RTP（Real-time Transport Protocol）と RTCP（RTP Control Protocol）に関する脆弱性を整理した。項目

8 は RTP を盗聴すると、代表的なオープンソースのパケット解析ソフトを利用して簡単にメディアを再生できる例を紹介した。項目 9 には偽装したメディアをミキシングしたり、置き換えられてしまう脆弱性を整理した。項目 10 には、あまり知られていないと思われる RTCP によるメディアの切断機能など、制御機能を悪用される脆弱性を整理している。

項目 11 は、RTP 上で転送されるメディアの符号化方式そのものについて、コーデックの脆弱性として資料をあたったが、直接、コーデックそのものの脆弱性は見当たらなかった。

ただし、工夫して作りこまれたコーデックのデータやパケットによって、機器の性能低下や暴走を誘発する例もある。このような不具合を起こしやすい脆弱性はその他のプロトコルに共通のものが多数あるため、項目 12 不具合を起こしやすいメッセージに対応できない問題として整理した。不具合を起こしやすいメッセージのうち、不正な形式のデータによって不具合を起こす製品の事例は、特に脆弱性の報告事例の大半を占めている。このことは、攻撃者から見れば、簡単な方法で広範囲の機器に応用が利き、効果をあげやすい手法であることの現れでもある。攻撃者の次のステップにあるとも言われる、ボット化を防ぐためにも、対策が急がれる分野である。この項目については特に製品の開発過程のそれぞれにおいての考察を記述している。

項目 13 から項目 16 は、SIP や RTP プロトコルそのものの脆弱性ではないが、製品が実装されるときに十分な設計や制御が行わなかったために発生する脆弱性を整理している。項目 13 は乱数であるべき SIP の Call-ID を偏った範囲の数値で生成したときの問題を、項目 14 は SIP の認証機能を正しく実装しないときの脆弱性を、項目 15 は SIP 端末が信用する SIP サーバや SIP プロキシサーバをきちんと識別しないときの脆弱性、項目 16 は SIP と RTP が協調して動作しないときの脆弱性を整理している。

項目 16 の SIP と RTP が協調動作できないときの問題は、SIP 特有であるとも言える。既存の代表的なプロトコルである HTTP は、接続の開始や認証、データ転送のすべてが同じ HTTP セッション上で行われるのがほとんどだが、SIP は制御のみを行い、メディアの転送は RTP が行う、という複数プロトコルでの役割分担がある。役割分担はさまざまな機能を取り込みやすいという特徴はあるが、きちんと連携した協調動作を行うためには別の仕様を定義する必要がある、というデメリットもある。こうした点から見ると、SIP/RTP を利用した製品開発には高いレベルのスキルが要求されるとも言える。

項目 17 は組込機器一般に言えることだが、IP 対応の組込機器ではリモートデバッガと呼ばれる、IP で接続した別のホストから機器内部のソフトウェアをデバッグする機能がよく使われることから、注目した。この脆弱性が残っている機器は非常に深刻な問題を起こす可能性がある。その他の関連する開発機能についても、注意が求められる。

項目 18 も IP ネットワーク関連機器に一般的に言えることだが、IP 電話機器や家庭用ルータ、ネットワーク製品に対して攻撃者が好んで利用する効率的な攻撃手法であるため、本報告書でも脆弱性として整理した。

項目 19 では電話番号や ID の一覧を収集されたり、機器の一覧や機器の構成情報を収集されるといった問題について整理した。ID や構成情報を収集されること自体は深刻度が低いが、攻撃者が効率的に攻撃を行うための準備作業として一般的に行われているため、脆弱性の一項目として整理した。なお、この項目内で迷惑電話についてとりあげたが、対策についてはさまざまな方法があり、現在も議論検討が行われているため、別資料の参照のみを提供している。

項目 20 では SIP 上で TLS を利用する際の問題として、電子証明書の利用方針をよく検討しておく必要がある点のほか、TLS の実装上の注意点についても整理した。例として TLS の第三者中継攻撃により、暗号通信路上の暗号情報が、第三者によっていったん復号されてしまう状況を示した。

項目 21 では、SRTP で用いる共通鍵を交換する方法に関する問題である。SRTP 用の共通鍵を SIP 上で暗号化せずに交換すると(SDES)、SRTP 用の共通鍵が攻撃者に盗聴され、RTP メディアが保護されなくなってしまう。ここでは SRTP 用の鍵交換方法をまとめつつ、DTLS-SRTP Framework について紹介している。

項目 22 では、SRTP で音声メディアを暗号化した場合でも、暗号前の元のパケット長やパケット数のトラヒック上の特徴から、暗号化前の音声を予想されることがある問題を紹介した。この問題は、攻撃者が暗号化のための鍵を入手する必要がなく、暗号方式の論理にも関係がない。

1.6. CVSS を基準にした深刻度 [参考値]

ネットワーク対応の製品、機器に関する脆弱性の情報は量が多い。大量の脆弱性情報の中で、対応すべき優先度をつけて、重大な脆弱性から順に対応する必要がある。そこで、脆弱性情報を提供する組織では、それぞれの脆弱性が及ぼす脅威の度合いを「深刻度」として数値化して提供している。深刻度は、影響の種類、容易さや範囲などの面から、脅威の度合いを数値化したものである。

共通脆弱性評価システム「CVSS」(Common Vulnerability Scoring System)は、脆弱性の深刻度を同一の基準のもとで定量的に評価する手法の確立と普及をめざし、米国の国家インフラストラクチャ諮問委員会（NIAC: National Infrastructure Advisory Council）のプロジェクトのもと、2004 年 10 月に原案が作成された。その後、CVSS 標準の管理母体として FIRST (Forum of Incident Response and Security Teams) が選ばれ、FIRST の CVSS-SIG (Special Interest Group)で利用促進活動や仕様の管理・改善が行われている。FIRST からは、2005 年 6 月に CVSS v1 が、2007 年 6 月に CVSS v2 が公開されている。

CVSS では次の 3 つの基準で脆弱性を評価している。

1) 基本評価基準(Base Metrics)
脆弱性そのものの特性を評価する基準。情報システムに求められる 3 つのセキュリティ特性、「機密性（Confidentiality Impact）」、「完全性(Integrity Impact）」、「可用性(Availability Impact）」に対する影響を、遠隔地(リモート)から攻撃可能かどうかといった基準で評価し、CVSS 基本値(Base Score)を算出する。
基本評価基準は製品ベンダーや脆弱性情報を提供する組織などが、脆弱性の固有の深刻度を表すことが可能で、この基準による評価結果は時間の経過、利用環境の異なりによって変化しない特徴があるとされている。

2) 現状評価基準(Temporal Metrics)
脆弱性の現在の深刻度を評価する基準。攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し、CVSS 現状値(Temporal Score)を算出する。
ベンダーや脆弱性を公表する組織などが、脆弱性の現状を表すために評価する基準であり、この基準による評価結果は、脆弱性への対応状況に応じ、時間が経過すると変化する。

3) 環境評価基準(Environmental Metrics)
製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準。攻撃を受けた場合の二次的な被害の大きさや、組織での対象製品の使用状況といった基準で評価し、CVSS 環境値(Environmental Score)を算出する。
製品利用者が脆弱性への対応を決めるために評価する基準であり、この基準による評価結果は、脆弱性に対して想定される脅威に応じ、製品利用者毎に変化する。

なお、IPA では脆弱性対策情報データベース JVN iPedia※1 や、脆弱性関連情報の調査結果のウェブサイトで CVSS v2 基本評価基準の評価値(基本値)を公表している。また、CVSS v2 そのものの詳細な基準、利用方法については「IPA - 共通脆弱性評価システム CVSS v2 概説※2」をご覧いただきたい。

※1 JVN iPedia
http://jvndb.jvn.jp/
※2 共通脆弱性評価システム CVSS v2 概説
http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html

1.7. 本報告書における CVSS 評価

本報告書においては、脆弱性の深刻度を評価する指標として「CVSS v2 基本値」のみを掲載した。CVSS v2 基本値とは、CVSS v2 の「基本評価基準」の評価値のことである。なお、CVSS v2 にある「現状評価基準」は時間の経過や技術の進歩に伴って評価基準が変化すること、「環境評価基準」は、対象システムを利用するエンドユーザの環境にあわせて評価されるべき基準であることから、本報告書の対応範囲外とした。また、本報告書の脆弱性項目 1 や項目 2 のように複数の脆弱性が含まれる項目については、最も深刻度が高い値のみを掲載した。更に、項目 18 や項目 19 のように、管理機能や ID、構成情報など共通したキーワードで括ることができる複数の脆弱性について取り上げ、それぞれの概要記載を行っている項目については CVSS 評価対象外としている。
読者におかれては、本報告書に記載されている CVSS v2 基本値は、当該脆弱性深刻度の評価を行う上での一つの参考指標であり、その深刻度は、時間経過や利用環境により変化するということをご認識いただいた上で、参考にしていただければ幸いである。

2. SIP 仕様解説

本章では、SIP に係わる脆弱性を理解する上で必要と考えられる SIP 関連プロトコルの概要について解説を行う。

2.1. SIP 関連プロトコル概要

SIP は、IP ネットワーク上でマルチメディアデータをエンドーエンド間で直接リアルタイムに双方向通信することを目的とした通信プロトコルである。IETF の SIP ワーキンググループで提案され、現在は RFC3261 で標準化されている。SIP によって実現するサービスには、IP 電話、ビデオ会議、インスタントメッセージ、プレゼンスなど多岐に渡る。

エンドーエンドでリアルタイム通信を行うためには、互いにマルチメディアデータを送受信する「セッション」を開設する必要があるが、SIP は、セッション開設のための通信相手を特定し、発信／着信／切断を実現するための「シグナリング」と呼ばれる機能を提供する。シグナリング以外の機能については他のプロトコルと組み合わせて実現する。例えば、マルチメディアデータの送受信自体は、RTP などのリアルタイム転送プロトコルを使用し、マルチメディアセッションの IP アドレス／ポート番号、データ圧縮方式などの交換については SDP（Session Description Protocol）を使用する。また、SIP はトランスポート層の上位に位置するアプリケーションプロトコルであり、さまざまなネットワーク構成に柔軟に対応できるよう、UDP および TCP のトランスポートに対応する。

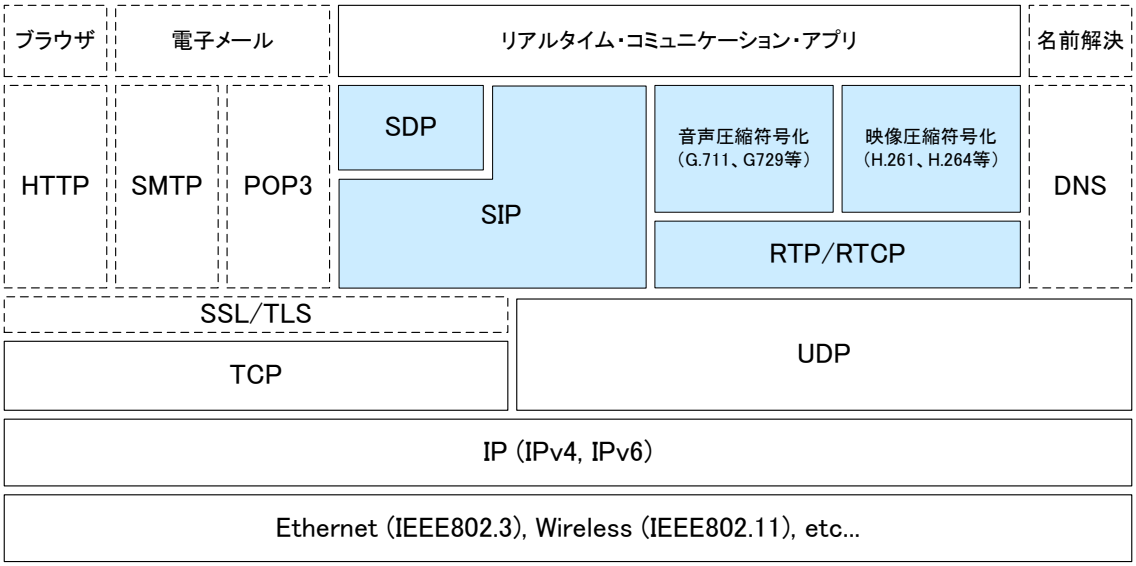


図 Ⅱ-1-2 プロトコルの位置付け

SIP は HTTP をベースにしたテキストベースのプロトコルであり、「解析が容易で開発がスムーズ」、「拡張性が優れている」などの特徴を持つ。

SIP の主な機能として、「呼制御」「登録」「プレゼンス」「インスタントメッセージ」の各機能を提供する。

表 Ⅱ-2 プロトコルの位置づけ

機能	機能概要
呼制御	• メディアに依存しない“コール”の制御 • 転送、会議、フォーク(SIP リクエストの複数宛先への分岐)などの様々な付加サービスの実現
登録	• SIP 端末からの位置(アドレス)情報登録による名前解決 • SIP 端末の認証
プレゼンス	• SIP 端末からの位置(アドレス)情報登録による名前解決 • SIP 端末の認証
インスタントメッセージ	• シグナリングセッション上でのデータ交換 • シンプルなメッセージ交換

RTP は、音声や動画などのデータストリームをリアルタイムに配送するためのデータ転送プロトコルであり、通常は RTCP による通信状態レポート（実効帯域幅や遅延時間など）と一体で利用される。RTCP は IP マルチキャストを用いた音声や動画通信を行なう様々なアプリケーションに実装されており、データストリームの受信者が RTCP パケットを定期的に送信することで、ストリーミングサーバは、通信状態に合わせて RTP で送信するデータの品質を調整して送信する。なお、RTP は UDP のみに対応しており、パケットロス対策や伝送時間保証などは行われていない。

2.2. SIP ネットワークの構成要素

SIP ネットワークは、SIP ユーザエージェント（UA）と複数種類の SIP サーバとにより構成される。

SIP UA は SIP の端末（クライアント）デバイスであり、SIP によりメディアセッションを確立し、メディアの送受信などの処理を行う。SIP を利用した IP 電話機やソフトフォン、テレビ会議端末、SIP ゲートウェイ装置などが SIP UA に該当する。SIP UA はリクエスト／レスポンスの関係により、UAC（User Agent Client）と UAS（User Agent Server）に区分され、その時々に応じて UAS または UAC として振舞う。以降、本報告書では、SIP UA を「SIP 端末」と記載する。

表 Ⅱ-3 UAC と UAS

UAC（User Agent Client）	SIP リクエストを生成し送出する側
UAS（User Agent Server）	受け取った SIP リクエストを処理し、レスポンスを生成・送出する側

一方、SIP サーバは SIP 端末間セッション確立の仲介や支援をする装置であり、SIP ではその役割ごとにサーバの種類が分けられている。

表 Ⅱ-4 SIP サーバの種類と機能

SIP サーバ	機能
登録サーバ (Registrar, Registration Server)	SIP 端末からの登録を受け付け、ロケーションサーバへ位置情報(IP アドレスなど)を登録する
ロケーションサーバ (Location Server)	SIP 端末の位置情報(IP アドレスなど)を管理する(データベースサーバなど)
プロキシサーバ (Proxy Server)	SIP 端末間の SIP リクエストとレスポンスを中継する
リダイレクトサーバ (Redirect Server)	SIP 端末からのリクエストに、正しい宛先を指定して返送する
プレゼンスサーバ (Presence Server)	SIP 端末からのプレゼンス情報を受け付けて蓄え、配信する

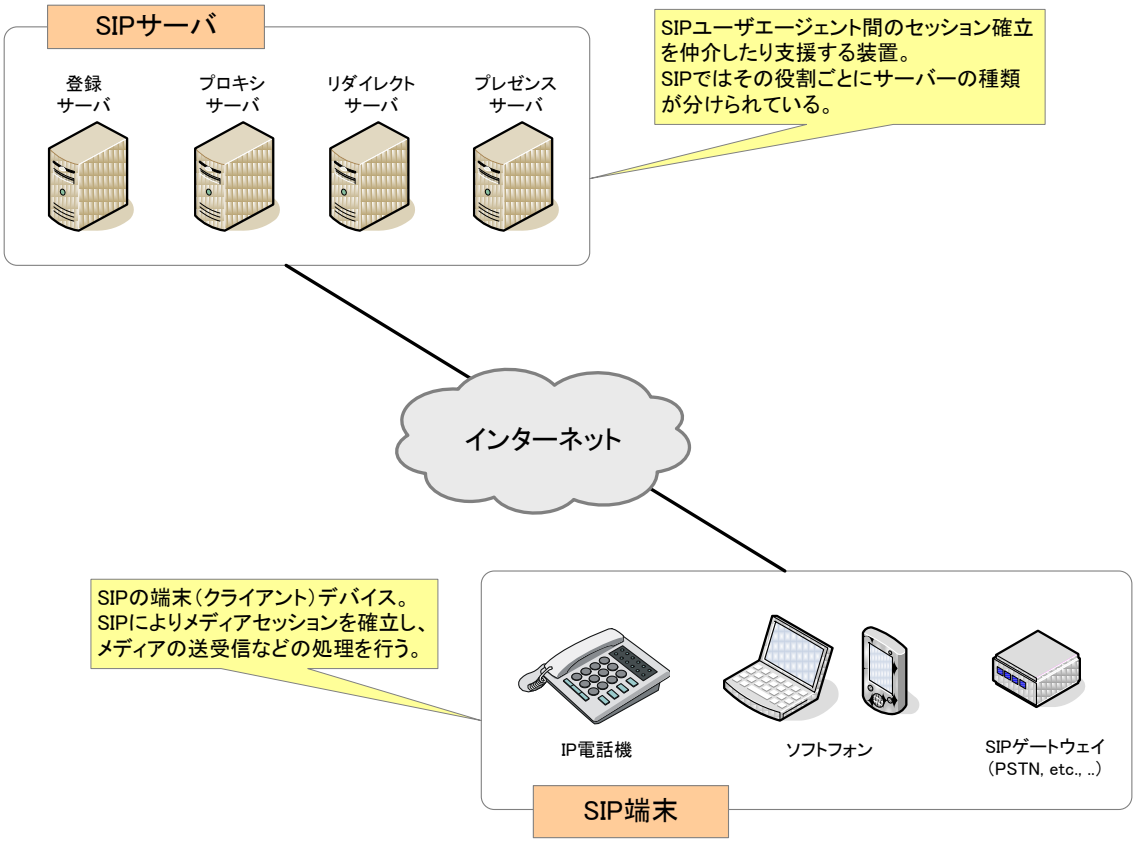
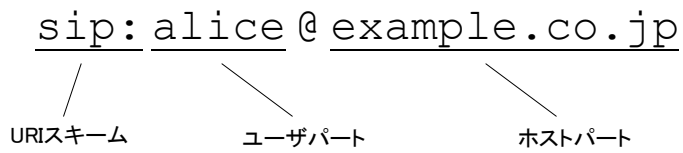


図 Ⅱ-1-3 SIP ネットワークの構成要素

各 SIP サーバは、図Ⅱ-2 のように連携してシステムを構成する（各 SIP サーバは、物理的に 1 台のサーバで実現することも可能）。SIP メッセージ中で送信元や宛先の指定には、世界中のリソースを一意に識別することができる SIP URI（Uniform Resource Identifier）と呼ばれる識別子が用いられる。Web の参照で利用される「http://www.example.co.jp/」などの URL（Uniform Resource Locator）も URI の一種であり、SIP の URI は「sip:」「sips:」により始まり、次の形式により表記される。



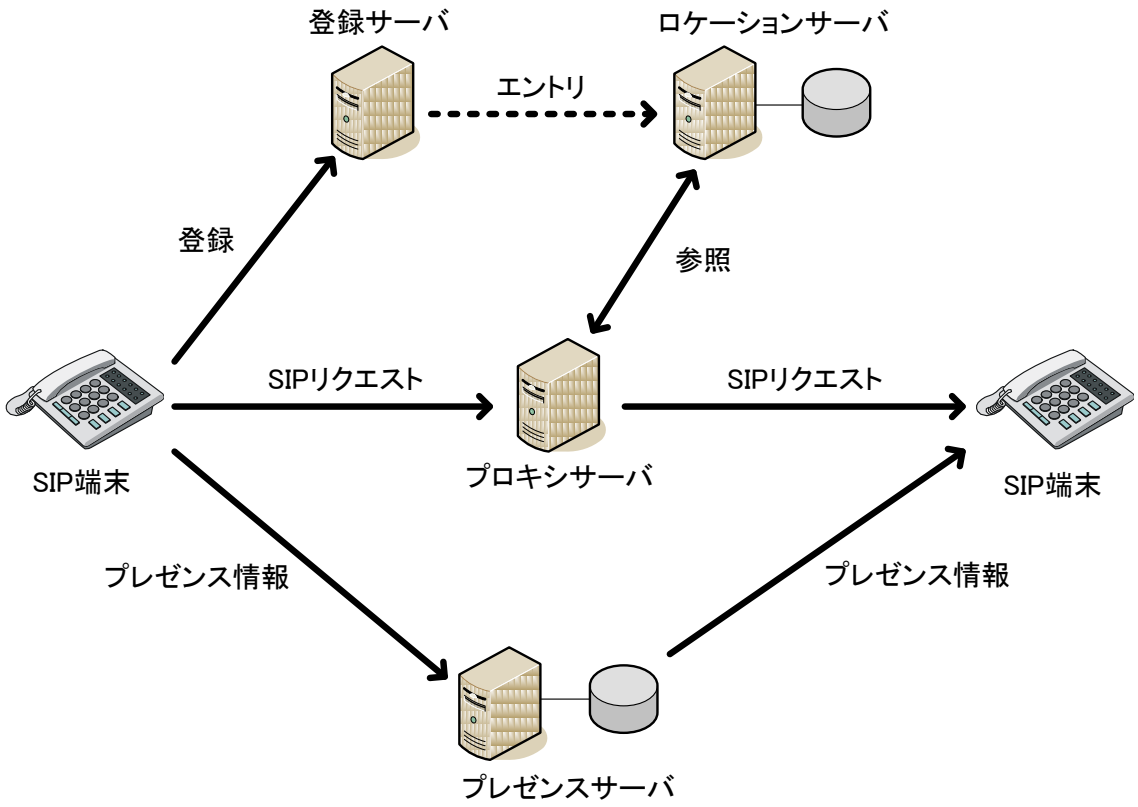


図 Ⅱ-1-4 SIP サーバの構成

2.3. 基本的なメッセージ形式

SIP の通信は HTTP をベースにしたプロトコルでメッセージをテキスト形式で表現する。そのため、人間が判読し易いので開発が比較的容易で、各種の機能拡張にも柔軟に対応できるというメリットを持つ。

SIP のメッセージは、図Ⅱ-4 のように「スタートライン」「ヘッダ」「ボディ」に分ける

ことができる。SIP のメッセージは、リクエストまたはレスポンスのいずれの場合でもその構造は変わらないが、スタートラインについてはそれぞれ「リクエスト行」または「ステータス行」と呼ばれる。なお、SIP メッセージの各構成要素とその役割は表Ⅱ-4 に示すとおりとなる。

```
INVITE sip:bob@biloxi.com SIP/2.0                          ←スタートライン
Via: SIP/2.0/UDP pc33.atlanta.com                            （リクエスト行）
  ;branch=z9hG4bK776asdhds
To: Bob <bob@biloxi.com>
From: Alice <alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE                                        ←ヘッダ
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 147
                                                           ←空行
v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=Session SDP
c=IN IP4 pc33.atlanta.com                                  ←ボディ
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

図 Ⅱ-1-5 SIP メッセージの概要（リクエスト）

```
SIP/2.0 200 OK                                             ←スタートライン
Via: SIP/2.0/UDP server10.biloxi.com                         （ステータス行）
  ;branch=z9hG4bKnashds8;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com
  ;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com                          ←ヘッダ部
  ;branch=z9hG4bK776asdhds ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131
                                                           ←空行
（以下省略）                                                ←ボディ
```

図 Ⅱ-1-6 SIP メッセージの概要（レスポンス）

表 Ⅱ-5 SIP メッセージの構成要素

SIP メッセージ構成要素		内容
スタートライン	リクエスト行	リクエストメッセージの先頭に記載し、INVITE（招待）、ACK（承認）などの SIP メソッド（命令）を記述する。
	ステータス行	レスポンスメッセージの先頭に記載し、200 OK（リクエストの受け入れ）、100 Trying（試行中）などのレスポンスコードで、リクエストの処理ステータスを示す。
ヘッダ		From（メッセージの送信元）、To（宛先）などのヘッダフィールドに、メッセージ関する情報を記述する部分。複数のヘッダフィールドを指定することができる。
空行		ヘッダ部とボディ部を区切るための空行。
ボディ		メッセージの本文（空の場合もある）。 INVITE メッセージでは、SDP に従って、使用できるメディアやパラメータなどを記述する。

「INVITE」のようなリクエスト行の先頭の記述は、「SIP メソッド」と呼ばれ、SIP メソッドは SIP のプロトコルで表Ⅱ-5 のように規定されている。SIP 端末は、相手に要求する制御内容に適した SIP メソッドをリクエスト行に記述する。

表 Ⅱ-6 SIP メソッド

SIP メソッド	内容
INVITE	セッションの確立
ACK	セッションの確立の確認
BYE	セッションの終了
CANCEL	セッションの確立キャンセル
REGISTER	登録
OPTIONS	サポート機能問い合わせ
PRACK	暫定応答の確認
INFO	セッション内の情報通知
SUBSCRIBE	状態情報の要求
NOTIFY	状態情報の通知
MESSAGE	テキストメッセージ等の送信
REFER	リクエストの送信指示
UPDATE	セッションの変更
PUBLISH	状態情報の通知

SIP では、レスポンスメッセージの中で受け取ったリクエストが「正常に処理された」または「エラーとなった」などの応答内容を 3 桁のレスポンスコードで表現する。SIP のレスポンスコードは、HTTP/1.1 のレスポンスコードの一部を拡張して表現され、表Ⅱ-6 に示すように 100 番台ごとに意味付けが分けられている。

表 Ⅱ-7 ステータスコード

レスポンスコード	区分	内容
1xx（100 番台）	暫定応答	リクエストを受信し、処理中である。 例：100 Trying、180 Ringing 等
2xx（200 番台）	成功応答	リクエストが理解され、受け入れられた。 例：200 OK、202 Accepted
3xx（300 番台）	リダイレクト応答	リクエストを完了するために、更なる処理が必要。 例：300 Multiple Choices、301 Moved Permanently 等
4xx（400 番台）	クライアントエラー応答	リクエストの書式が間違っていたか、このサーバでは処理できない。 例：400 Bad Request、401 Unauthorized 等
5xx（500 番台）	サーバエラー応答	サーバでのリクエスト処理に失敗した。 例：500 Server Internal Error、501 Not Implemented 等
6xx（600 番台）	グローバルエラー応答	リクエストをどのサーバでも処理できない。 例：600 Busy Everywhere、603 Decline 等

2.4. SIP の基礎シーケンス

ここでは、SIP メッセージとして代表的な「登録（REGISTER）」「セッション確立（INVITE）」「セッション切断（BYE）」「着信拒否」「発信取り消し（CANCEL）」の 5 例について、一連のシーケンスを記載する。

2.4.1. 【登録（REGISTER）】

SIP において移動先でも利用できるモビリティを実現するために必要なものが登録サーバへの登録（REGISTER）である。登録は、SIP 端末が登録サーバに対し REGISTER リクエストを用いて行い、SIP 端末自身の SIP URI と IP アドレスを登録する。通常、登録サーバは SIP 端末の登録を時間管理（有効時間超過で登録抹消）し、SIP 端末は登録有効時間内で再登録する。登録が有効な状態は「レジストレーション」と呼ばれる。

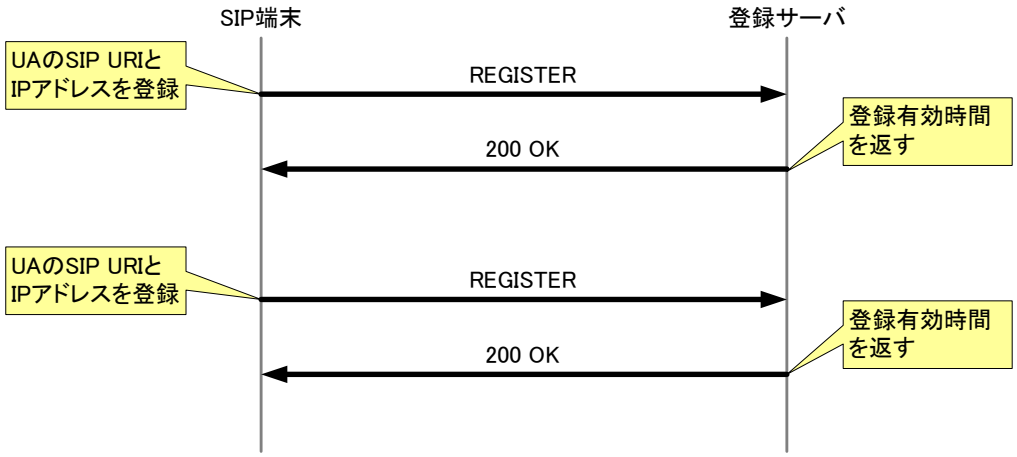


図 Ⅱ-1-7　REGISTER シーケンス

2.4.2. 【セッション確立（INVITE）】

音声、映像などのマルチメディアセッションは SIP 端末－SIP 端末間で、INVITE － 200 OK－ ACK の 3 ウェイ・ハンドシェイクにより確立される。INVITE リクエストに対する 1xx レスポンスは暫定応答（最終的な結果ではなく途中経過を表す）であり、最終的な受付結果ではない。これは、INVITE リクエストを受けた SIP 端末（UAS）は、200ms 以内に何らかのレスポンスを返さなくてはならないという規定に沿うための動作である。

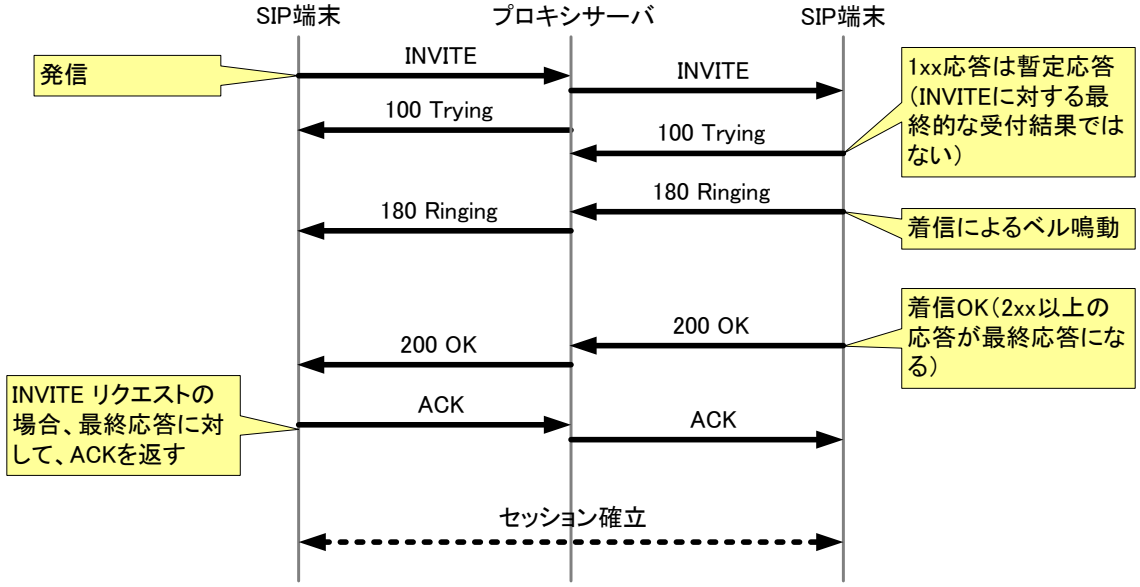


図 Ⅱ-1-8　INVITE シーケンス

2.4.3. 【セッション切断（BYE）】

INVITE / 200 OK / ACK で確立したセッションは、切断するという操作により正しくセッションを切断できなくてはならない。そためのリクエストが BYE リクエストとなる。発信側、着信側のどちらでも BYE リクエスト を送出可能であり、BYE リクエストを受け取り、200 OK が返されるとセッションが切断される。

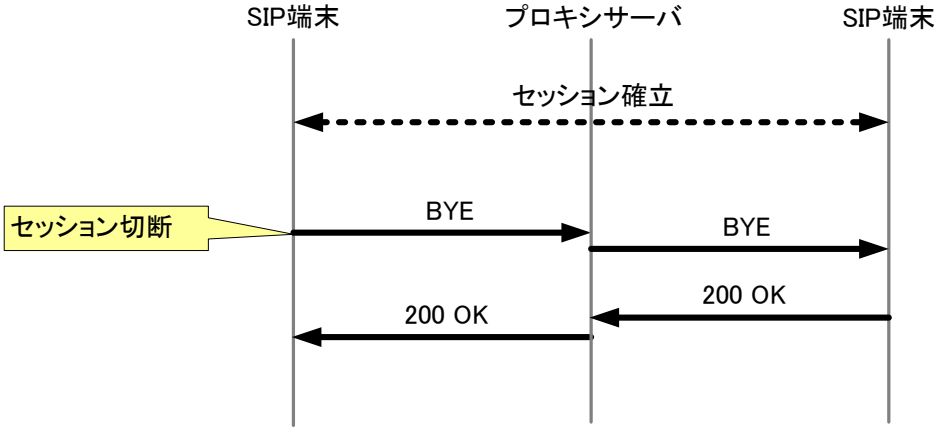


図 Ⅱ-1-9　BYE シーケンス

2.4.4. 【着信拒否】

着信拒否は INVITE によるセッション確立要求に対して 3xx 以上の最終応答によって、拒否を行う。このように、セッション確立にならない場合であっても INIVTE－最終応答－ACK の動作により実現される。

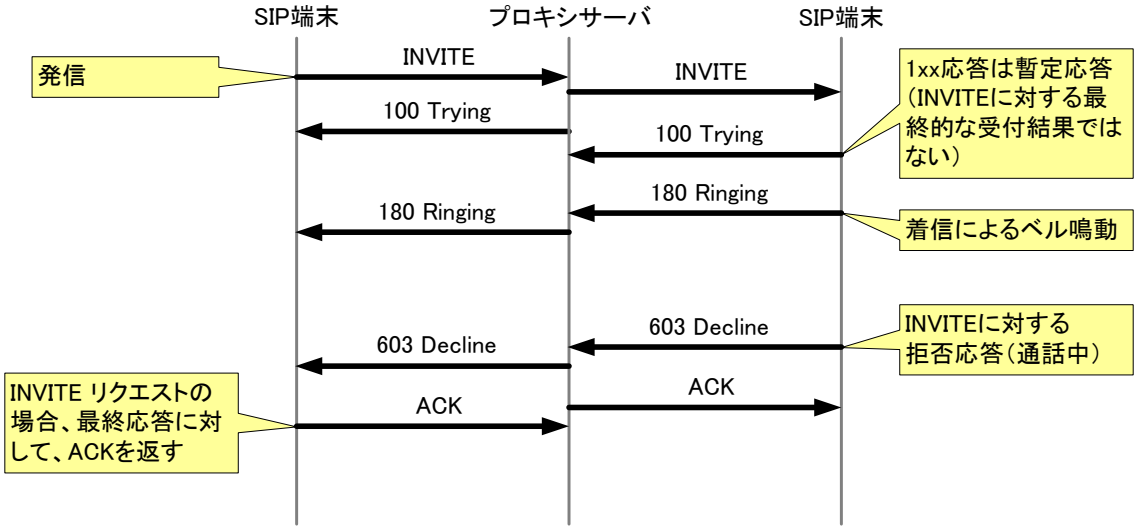


図 Ⅱ-1-10 着信拒否シーケンス

2.4.5. 【発信取り消し（CANCEL）】

CANCEL リクエストは、セッションが成立する前に発信を取り消す際に利用される。CANCEL リクエストが送信されると、200 OK によって CANCEL リクエストに対する成功応答を行い、INVITE リクエストに対する取り消し応答は、487 レスポンスで最終応答を行い、これに対し ACK を返して発信の取り消しとなる。

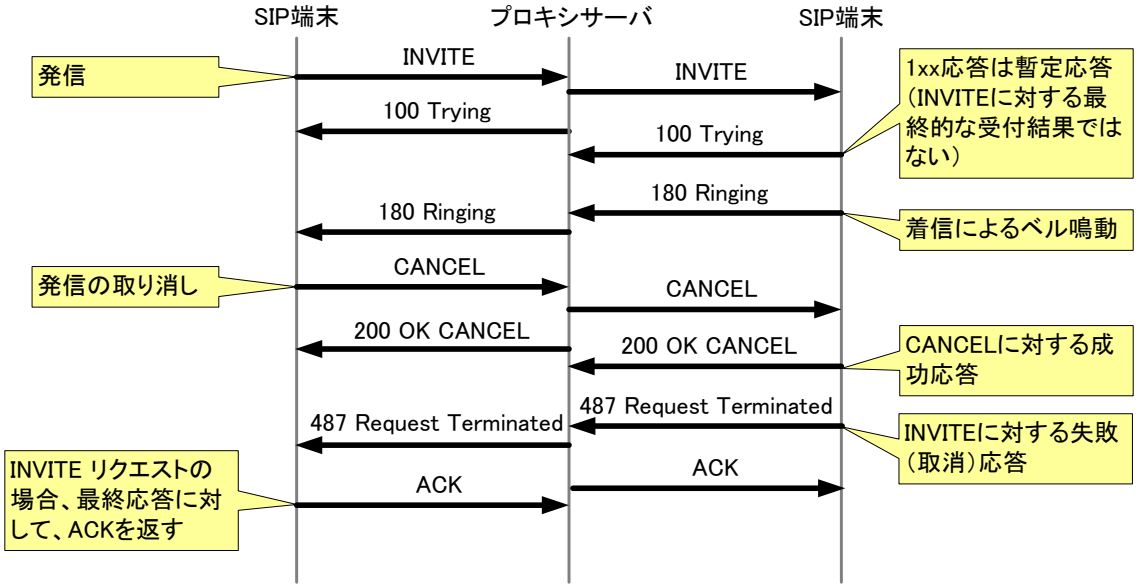


図 Ⅱ-1-11 CANCEL シーケンス

2.5. SIP の認証

SIP では、各リクエストに対して送信元が正しいユーザであるかを、「認証」する機能を持つことができる。認証には HTTP ダイジェスト認証方式と呼ばれるチャレンジ・レスポンス方式の認証メカニズムを基本的に採用している。ダイジェスト認証は、基本認証（Basic 認証）に置き換わるものとして、HTTP/1.1 から新たに提案された認証方法で RFC 2617 によって規定されている。

HTTP ダイジェスト認証方式では、認証情報を要求するサーバから SIP 端末側のメッセージに WWW-Authenticate ヘッダにチャレンジ値を含めて送信する。この時の認証を要求するエラーメッセージは「401 Unauthorized」となる。これに対し、認証される側の SIP 端末からは、受信したチャレンジ値からレスポンス値を算出し、送信するメッセージの Authorization ヘッダに認証情報を含めて送信する。なお、レスポンス値の算出には、ユーザ名とパスワードから計算が行われる。

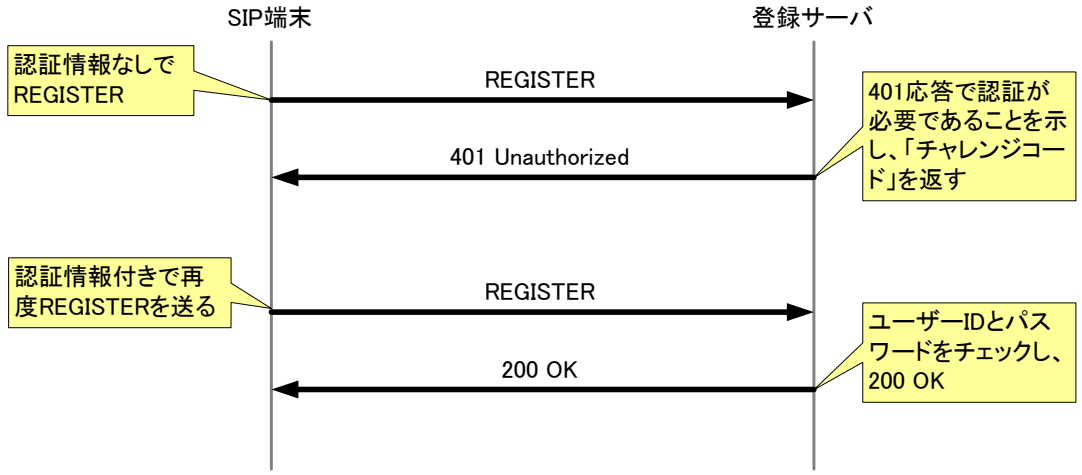


図 Ⅱ-1-12 レジストラ認証

401 Unauthorized （HTTP ダイジェスト認証チャレンジ）

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pc33.example.co.jp:5060;branch=z9hG4bK7e010369
From: sip:alice@example.co.jp;tag=1008141161
To: sip:alice@example.co.jp;tag=1089012396910
Call-ID: 2c8e0369-75671f481397401d8f6508d51ae9a1dc@pc33.example.co.
jp
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="unknown",       nonce="8a8aee697577e
338dae62dc442149b8d",
     opaque="", qop="auth", stale=FALSE, algorithm=MD5
Content-Length: 0
```

図 Ⅱ-1-13 REGISTER 時の認証要求の例

REGISTER （HTTP ダイジェスト認証レスポンス）

```
REGISTER sip:172.17.0.20:5060 SIP/2.0
Via: SIP/2.0/UDP pc33.example.co.jp:5060;branch=z9hG4bK6ee70373
Max-Forwards: 70
To: sip:alice@example.co.jp
From: sip:alice@example.co.jp;tag=1008141161
Call-ID: 2c8e0369-75671f481397401d8f6508d51ae9a1dc@pc33.example.co.
jp
CSeq: 2 REGISTER
Contact: sip:alice@pc33.example.co.jp:5060;expires=3600
Authorization: Digest realm="unknown",
      nonce="8a8aee697577e338dae62dc442149b8d",
      opaque="", algorithm=MD5, qop=auth, cnonce="1FBB0373",
      nc=00000001, uri="sip:172.17.0.20:5060", username="alice",
      response="907228c79a27a566ca47b41c2a6b72de"
Content-Length: 0
```

図 Ⅱ-1-14 認証情報付き REGISTER の例

SIP の認証においてプロキシサーバが存在する場合、プロキシサーバが SIP 端末に認証を要求することで、認証情報の転送を行うことができる。例えば、認証情報なしで INVITE メッセージを受け取ったプロキシサーバは、送信側の SIP 端末に「407 Proxy Authentication Required」のメッセージを送ることで認証情報の送信を促し、受け取った認証情報を相手側の SIP 端末に認証情報をフォワードするという動作を行う。

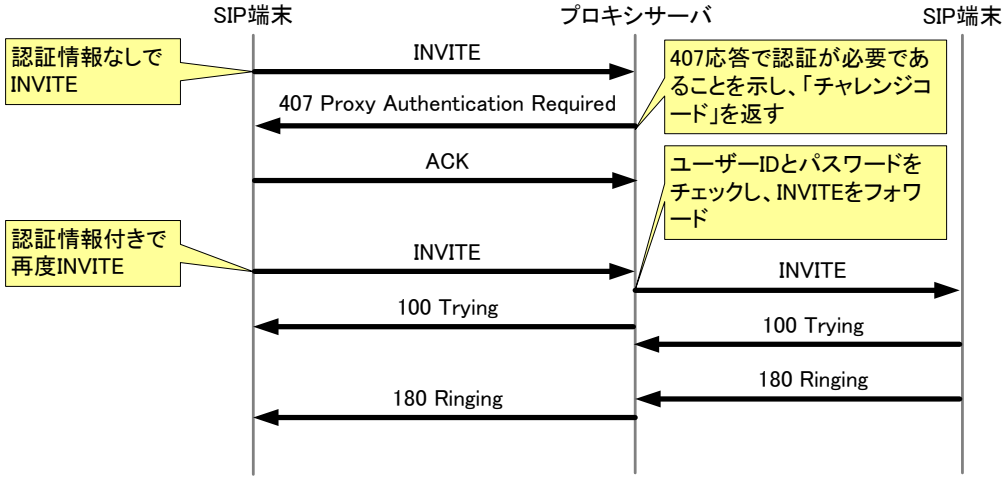


図 Ⅱ-1-15 プロキシ認証

SIP 端末が通信相手の SIP 端末に対して認証を要求するということも可能である。レジストラ認証、プロキシ認証と組み合わされたシーケンスとなり、その場合の認証を要求するエラー応答には「401 Unauthorized」が用いられる。

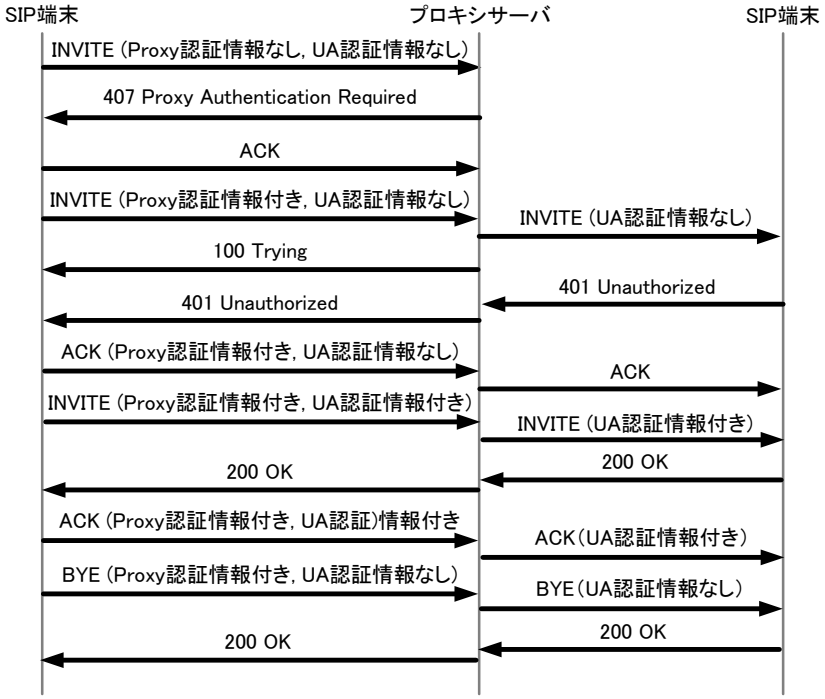

SIP端末
プロキシサーバ
SIP端末
INVITE (Proxy認証情報なし, UA認証情報なし)
407 Proxy Authentication Required
ACK
INVITE (Proxy認証情報付き, UA認証情報なし)
INVITE (UA認証情報なし)
100 Trying
401 Unauthorized
401 Unauthorized
ACK (Proxy認証情報付き, UA認証情報なし)
ACK
INVITE (Proxy認証情報付き, UA認証情報付き)
INVITE (UA認証情報付き)
200 OK
200 OK
ACK (Proxy認証情報付き, UA認証)情報付き
ACK(UA認証情報付き)
BYE (Proxy認証情報付き, UA認証情報なし)
BYE(UA認証情報なし)
200 OK
200 OK

図 Ⅱ-1-16 端末認証

3. SIP 関連システムの利用形態

本章では、SIP を用いたシステム利用形態として代表的な利用例について解説を行う。

3.1. IP 電話(VoIP)での利用

3.1.1. 【企業内での IP 電話利用】

IP 電話としての利用は、SIP が利用される最も典型的な利用形態である。近年では、オフィス内の電話システムが IP 電話化されているということも珍しいことではなくなってきた。従来の PBX を用いた電話システムを SIP サーバによる IP 電話システムに置き換えることで、情報ネットワークと電話ネットワークを統合した IP ネットワークによるネットワークインフラを構築する形態である。公衆電話網への接続は、オフィス内に設置された回線収容装置と呼ばれる機器などにより、IP 電話網と既存の電話網(PSTN: 公衆電話交換回線網)との接続を可能とする。

なお、この場合のユーザ利用端末は電話機の形をした IP 電話機だけでなく、PC に IP 電話ソフトウェアをインストールして利用するソフトフォンの形態や屋外では携帯電話として利用でき、オフィス内では、無線 LAN を利用して SIP サーバに接続する SIP 対応携帯端末など様々な利用形態での利用が進んでいる。

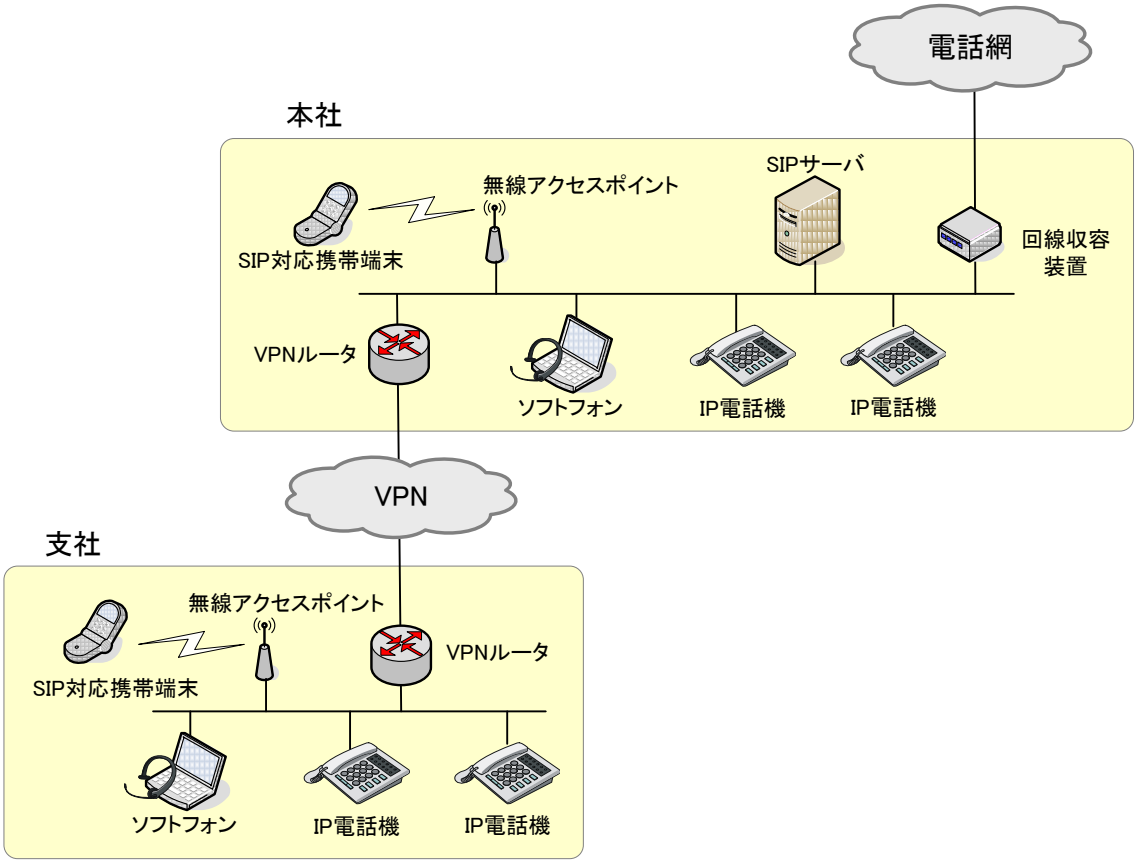


図 Ⅲ-1-17 企業内での IP 電話利用

3.1.2. 【一般向け IP 電話サービス】

下図は、ISP や通信事業者が提供する IP 電話サービスにおける利用形態である。ユーザの利用する SIP サーバは、ISP や通信事業者のネットワーク内に設置され、ユーザ宅内に設置された VoIP アダプタや IP 電話機が SIP を用いたセッション制御を利用して IP 電話を利用するというサービスである。このようなサービスにおいては、サービス提供者側で一般電話網(PSTN: 公衆電話交換回線網)とのプロトコル変換を行った上での相互接続を行うことで、一般電話との通話を可能としている。このようなサービスにおいては、近年、ソフトフォンを用いた IP 電話サービスなども提供されてきている。

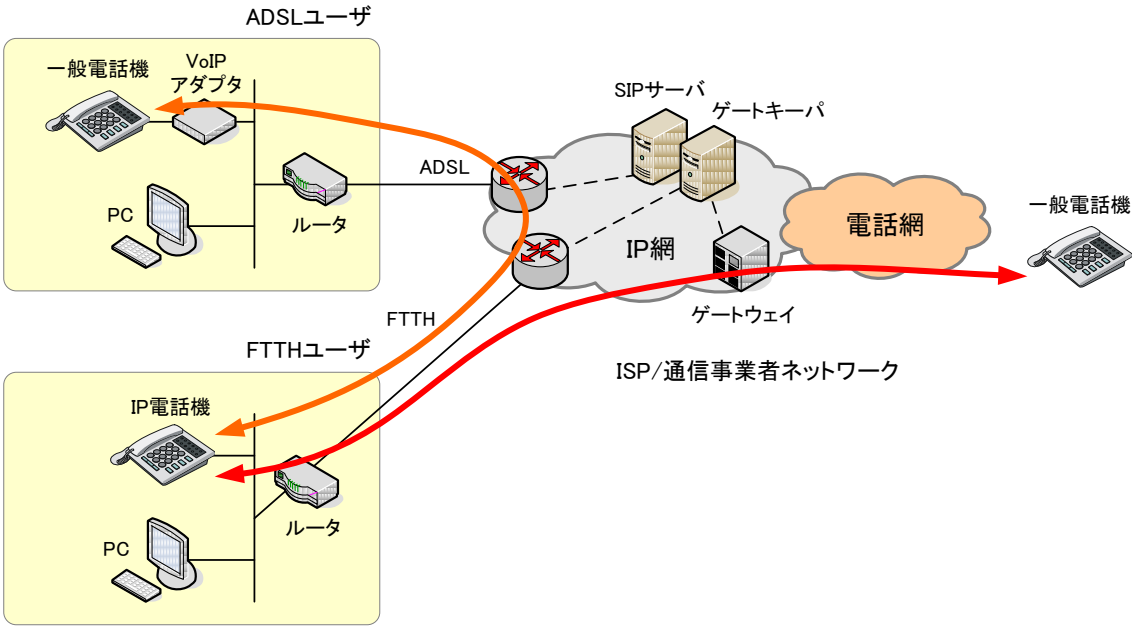


図 Ⅲ-1-18 一般向け IP 電話サービス

3.2. インスタントメッセージとプレゼンスでの利用

インスタントメッセージ（Instant Message：IM）は、専用のソフトウェアを用いてインターネット上でテキストメッセージの交換を実現するサービスである。これらのサービスは、多くのソフトウェアベンダから提供されており、現在は、インターネット上での代表的なコミュニケーション・ツールの一つとなっている。

IM サービスでは SIP の機能を拡張し、リアルタイム・コミュニケーションを実現するために規定された SIMPLE（SIP for Instant Messaging and Presence Leveraging Extensions）などのプロトコルを用いて実現している。元々、SIP ではユーザの登録機能が定義されており、この登録情報はプレゼンス情報として用いることができるため、SIP 自体がプレゼンスサービスに向いていると言うことができる。しかし、実際にはアプリケーションごとに独自拡張されている場合が多く、相互接続が難しいという現状もある。

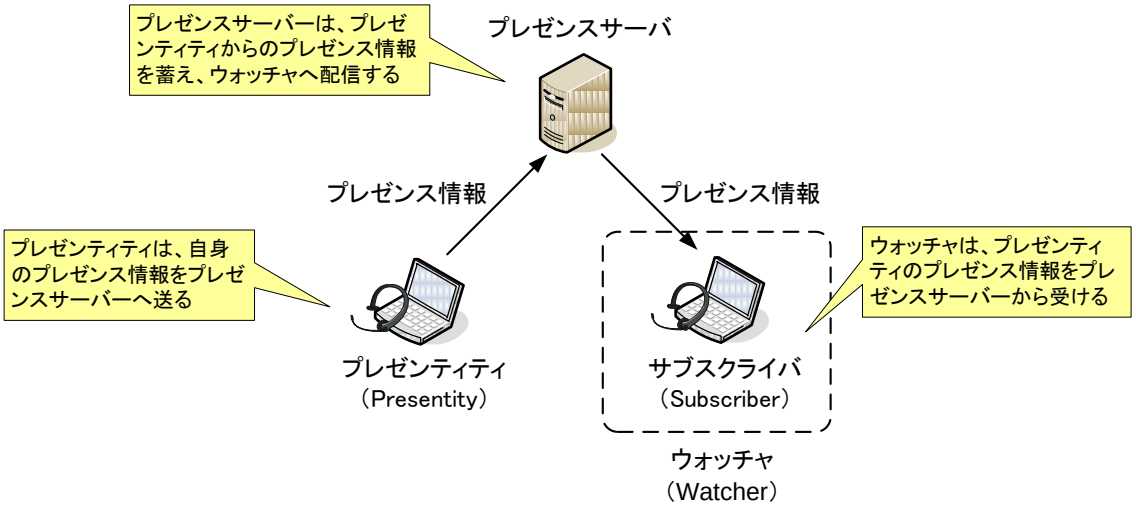


図 Ⅲ-1-19 プレゼンスでの利用

3.3. 通信事業者の提供する NGN での利用

NGN（Next Generation Network）とは、IP ネットワークをベースとした次世代の通信事業者のネットワークのことを言い、そのコア技術として SIP が利用されている。NGN では電話サービスだけでなく、マルチメディア系のサービスも含めて統一的に提供するためのアーキテクチャとして、第 3 世代携帯電話の標準化組織である 3GPP が策定した IMS（IP Multimedia Subsystem）を採用している。その IMS の中で、シグナリング・プロトコルとして SIP が採用されている。現在、国内外の通信事業者が NGN への移行に向けた取組みを展開しており、SIP は益々身近なプロトコルとなると同時に高い信頼性を求められていくことになる。

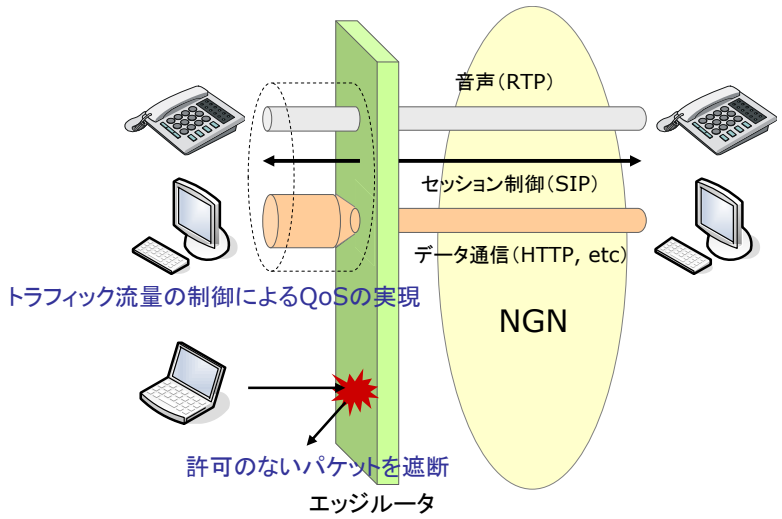


図 Ⅲ-1-20 NGN における SIP の利用

3.4. モノとモノをつなぐ通信での利用

ネットワーク接続機能を持ったハードディスクレコーダーなどに代表されるネット家電の接続においても、SIP の利用が検討されている。ネット家電がホームネットワークに接続する際の相互接続性の向上と安全な通信の実現に向けた直接通信とネット家電の遠隔制御を実現する仕組みである。いずれも、SIP をベースにセキュリティ機能を拡張した通信方式により実現されようとしている。

ネット家電間の直接通信では、暗号化されたシグナリングチャネル上で SIP のリクエストを拡張した方式で認証サーバを介した認証を受けた後、認証サーバを介さずに直接、ネット家電間で暗号化された直接通信を行う。

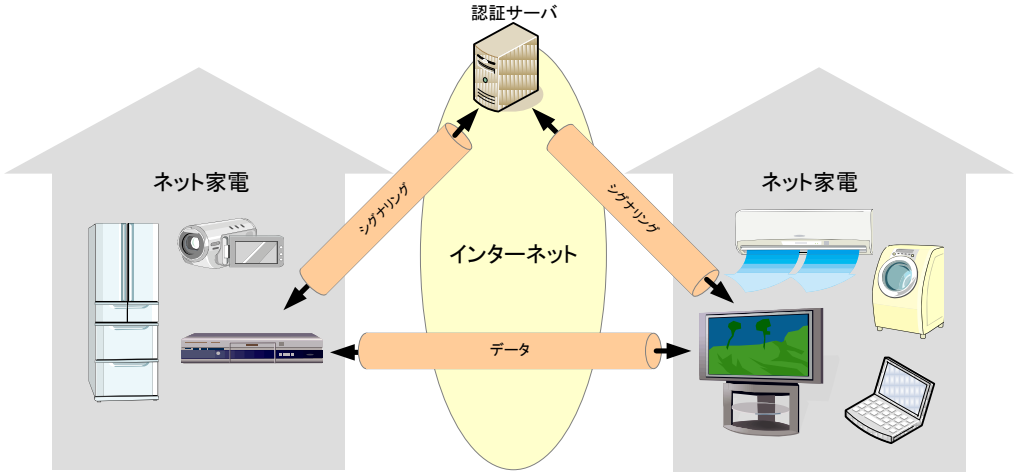


図 Ⅲ-1-21 ネット家電間の直接通信

また、ネット家電の遠隔制御では、宅外からネット家電の操作や監視、ネット家電から宅外への状態通知を実現する。シグナリングチャネルを利用するネット家電の操作や監視には SIP のプレゼンス機能が利用されている。

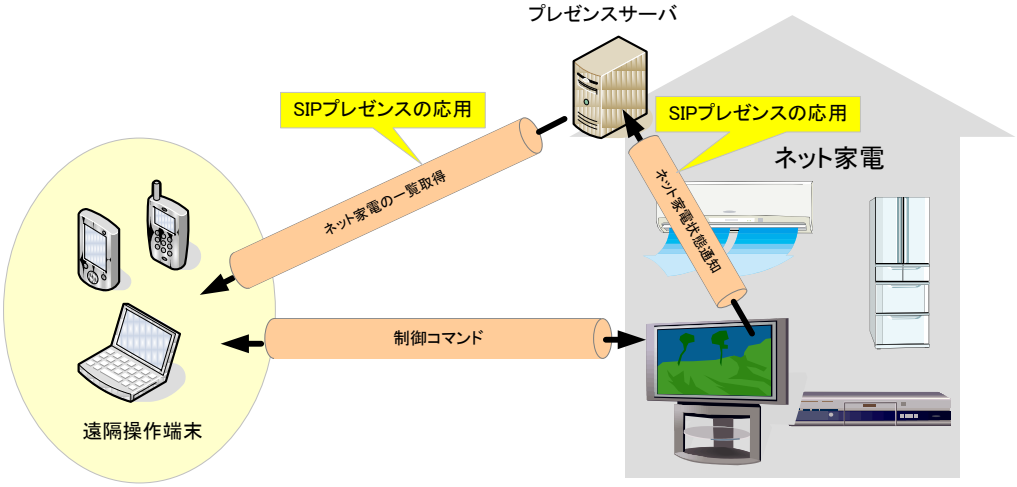


図 Ⅲ-1-22 ネット家電の遠隔制御

4. 本報告書記載における前提等

本章では、本報告書「脆弱性項目解説」の記述にあたり前提とした諸条件や読み進める上での留意点などについて記述を行う。

4.1. SIP プロキシサーバの省略

SIP による通信の一般的なモデルは図Ⅳ-1 にあるような「台形モデル」と考えることができる。このモデルは、以下の 4 つのホストが SIP のリクエストとレスポンスを送受信している例となっている。

・発信側 SIP 端末(アリスのソフトフォン)
・アリスの属する SIP サービスドメイン(atlanta.com)のプロキシサーバ
・ボブの属する SIP サービスドメイン(biloxi.com)のプロキシサーバ
・着信側 SIP 端末(ボブの SIP フォン)

一般に、この送受信間に SIP のプロキシサーバが複数入ることが許されており、プロキシサーバが入ったことにより、メッセージの転送が増えたとしても、本質的な影響はない。逆に、発信側 SIP 端末と着信側 SIP 端末が直接 SIP リクエスト/レスポンスを送受信できるのであれば、間にプロキシサーバが一つも存在しなくてもやはり、本質的な影響はない。
本文書の解説の中では、図を簡単にするため SIP の脆弱性に直接影響しない場合はプロキシサーバを図中に描画しない場合が多いので注意されたい。

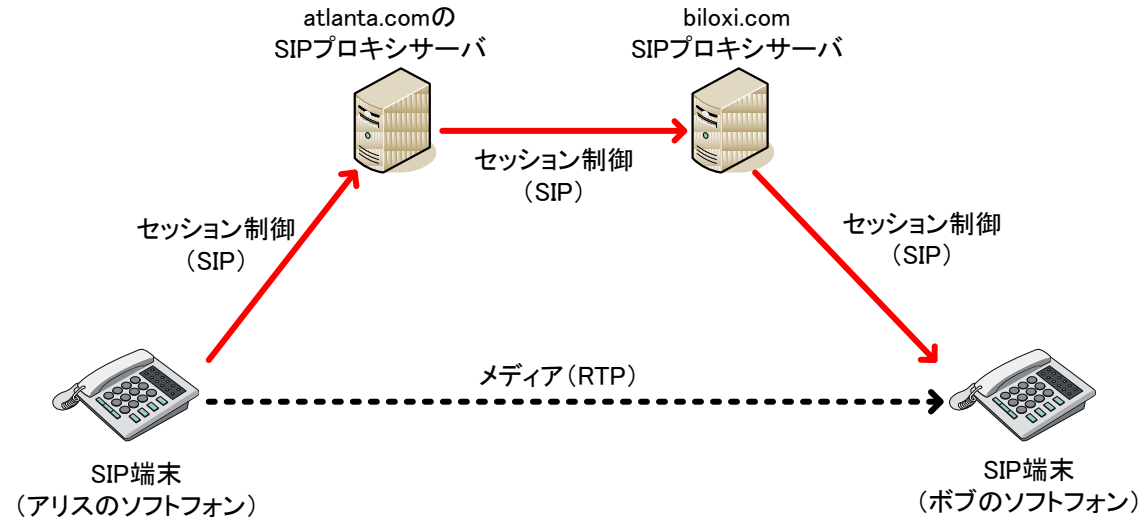


図 Ⅳ-1-23 SIP のセッションセットアップ例

4.2. 前提となる IP ネットワーク環境

本報告書では、広い意味での IP ネットワーク環境において SIP 関連プロトコルを利用した製品、機器を利用することを前提に脆弱性情報を収集した。広い意味での IP ネットワーク環境とは、以下のようなネットワークを含んでいる。

1) 固定または携帯型を含む、通信事業者が提供するインターネット接続サービスまたは VPN サービス網、特定用途サービス網
2) 一般企業がオフィスや工場内などで自営で運用する IP ネットワーク
3) ビルやホテル内などで提供される IP ネットワーク
   Ethernet スイッチや Ethernet ハブ(リピータ)を不特定多数が共用することがある
4) 公衆無線 LAN ホットスポット(無線 LAN 暗号化あり/なしの両方を含む)
5) インターネットカフェ(不特定多数が同じ Ethernet スイッチ/ハブを共用する)
6) 個人が家庭内や小規模オフィス(SOHO)に設置した IP ネットワーク
   暗号化されていない無線 LAN も含む

上記の広い意味での IP ネットワーク環境では、端末からネットワークへのアクセスが適切に制御されているとは限らない。また、ネットワーク機器の構成や無線 LAN の設定方法によっては、同一ネットワーク機器に接続する他の端末のパケットを容易になりすまし、中継、改ざんすることが可能な場合がある。特に、上記のような管理されていない IP ネットワークの問題は端末と SIP サーバの間などの、いわゆるネットワークのアクセス区間に顕著である。一方、SIP サーバと別の SIP サーバの間については、IMS や NGN ではコアネットワークと呼ばれているが、典型的な日本の IP 電話サービスではコアネットワーク部分は通信事業者が運用しており、安全な IP ネットワークが提供されているものと期待されている。ただし一般企業が利用する IP-PBX においては、SIP サーバ間の接続は一般のインターネット接続を経由することも想定され、導入時には注意が必要とされる。

なお、SIP を利用したインターネット上でのパソコン用通話サービスはすでにいくつか提供されている。

4.3. 攻撃手法に共通する前準備に関する記述

多くの脆弱性項目では、攻撃手法に共通する前準備として、IP パケットの盗聴、なりすまし、第三者中継を行うためのネットワーク環境の構築が必要となる。

物理的な方法としては、真正な利用者端末や SIP サーバ機器の間に、攻撃者が介入して中継を行うように、機器や配線を構成することである。例えば以下のような方法がある。

1) Ethernet タップや光分岐装置を利用して介入する
2) Ethernet スイッチのパケットミラーリング機能を利用する
3) ルータ装置、ブリッジ装置機能を擬似した装置を、配線して挿入する

このような物理的な方法は非常に安定して利用でき、試験機器が与える遅延やパケットロスなどの影響も小さい。そのため、詳細なパケットキャプチャや、品質を評価するための情報収集、多数の脆弱性項目の試験や確認、詳細な検討を前提とした検証作業などに適している。

また、ソフトウェアだけで対応するための方法もある。Ethernet 上の IP ネットワークでは、パケットの盗聴や改ざんを行うために、偽装した ARP パケットを送信して、他の特定の IP アドレス宛のパケットを自ホストの Ethernet インターフェースに届けさせることができる。この手法は ARP ポイズニングや ARP スプーフィングとして知られ、複数のツールや、別のツールの一機能として統合されている。ARP ポイズニングや ARP スプーフィングに関する解説については、IPA 発行の「TCP/IP に係る既知の脆弱性に関する調査報告書」※ “21. ARP テーブルが汚染される問題”を参照してほしい。

※ TCP/IP に係る既知の脆弱性に関する調査報告書
http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

アクセス用のネットワークについては無線 LAN の脆弱性も注意が必要である。特に無線 LAN の Ethernet フレームを暗号化する方式である WEP は、数時間から数十分で暗号化鍵を解析できるとされ、複数の自動解析ソフトウェアが公開されている。対策として WPA を利用する必要がある。

ソフトウェアによる方法は条件によって失敗することもあるが、専用の機器や装置が不要なため、手軽に実行できるメリットがある。無線 LAN のように移動先で試験しなければならないときや、特定の顧客やフィールドで試験を行わなければならないときに便利である。

なお、攻撃者がとる手法は一般的にソフトウェアを利用した方法が多いと考えられるが、ハードウェアや別のネットワーク機器を乗っ取って行う攻撃手法には、攻撃がまったく検知されないなどの、被害者側にとっての重大なデメリットがあるため、慎重な検討が必要である。

以上のような IP パケットの盗聴、なりすまし、第三者中継の準備手順や手法については、TCP/IP から下のプロトコル階層に強く依存する方法であるため、個別の脆弱性項目内では記述していない。詳細は IPA が発行する「TCP/IP に係る既知の脆弱性に関する調査報告書」などをご参照いただきたい。

4.4. 本文中で想定される SIP/RTP の利用方法

SIP は拡張性が高い反面、さまざまな利用方法、利用形態をとることができるため、ある程度の範囲内で利用方法を想定することが必要である。また、特に既存の電話網(PSTN: 公衆電話交換回線網)と相互接続する IP 電話システムや、IP-PBX では、PSTN への発信、発呼によって通信事業者から課金されることになるため注意が必要だ。

ここでは、本報告書で想定される SIP/RTP の利用方法をまとめている。本報告書執筆時点では、典型的な日本国内の IP 電話またはテレビ電話サービスに準ずるものとし、以下のように想定している。

1) SIP/RTP のトランスポートプロトコルには UDP を利用する
2) UDP は生の IP パケットペイロード上に載せられ、IPsec は使われていない
3) SIP サーバまたは SIP プロキシサーバは、SIP CANCEL リクエスト以外のすべての SIP リクエストに対して SIP 認証を要求する
4) SIP 認証は MD5 ダイジェスト認証が利用する
5) SIPS(SIP over TLS)は使われていない
6) SRTP(Secure RTP)は使われていない
7) SIP 端末はほぼ常時(1 時間おきなどに)、事前に設定された SIP サーバに SIP 端末を登録(REGISTER)する
8) SIP 端末への着信セッションは、SIP サーバ上の登録情報を参照して行われる

これらの SIP/RTP の利用方法が、「4.2 前提となる IP ネットワーク環境」で利用される、とお考えいただきたい。

4.5. 「もともと解決したいこと」と「脆弱性」 ～ 対策の考え方

本報告書では、それぞれの脆弱性対策を記述しているが、場合によってはそうした脆弱性対策が別の問題を引き起こすこともある。

例えば、前段で紹介した偽装 ARP パケットを利用した、別のホストの Ethernet インターフェースになりすます手法は、すでに一部の製品で利用されている。例えば、無停止で運用できる、高可用性(HA)を提供する製品や、代替のデフォルトルータを広報する機能(VRRP)では、偽装 ARP と同じしくみを利用して、デフォルトルータの切り替えや Ethernet インターフェースの故障時切り替え(Fail Over)を行っている。

例えばこのような偽装 ARP を Ethernet スイッチのセキュリティ機能を利用してすべて遮断すると、VRRP や HA 機能が利用できなることになる。そのため、既存の運用中のネットワークやシステムに対して、脆弱性対策を実施する際は、既存のサービスに問題を与えないか検討し、必要ならば代替案を用意することがある。また、場合によっては、設計開発の原点に立ち戻り、「もともと何の業務をコンピュータで実行したかった」ということを検討しなおすことも必要である。

すべての脆弱性に該当するわけではないが、特に SIP と RTP の標準仕様は実装して機能を提供することが先に進み、セキュリティは別のプロトコルやレイヤで解決することが想定されてきたため、ある面から見れば脆弱性であることが、別の面から見ると、別の機能やサービスを提供するための鍵であることもある。

脆弱性にはこのような二面性があることを理解して読み進めていただければ幸いである。

4.6. SIP 関連プロトコルの脆弱性の現状

SIP 関連プロトコルは拡張性が高く、容易に開発できる特徴があるが、もともと SIP そのものには、SIP の通信を保護する機能がまったくない。そのため、SIP の通信を盗聴して、特定の SIP 端末になりすましたり、SIP 認証のパスワードを解読しやすい面がある。また、メディアを転送する RTP にも、保護機能は事実上ないに等しく、音声やビデオのデータを簡単に盗聴できる。

また、実装の未熟さから、SIP と RTP のそれぞれ別の処理を扱うモジュールの間での統合がとれていない問題がある。その結果として、利用者への認証処理がなかったり、認証結果のひきつぎが行われなかったりすることで、不正な利用を許してしまう問題がある。

本報告書執筆時点では、SIP 関連プロトコルの通信を保護するための標準として、TLS や SRTP などが存在するが、実際に利用できる製品はまだ豊富にそろっているとは言えない。そのため、SIP 関連プロトコルの通信を保護するには、SIP 以外の対策方法に頼らなければならないのが現状である。

こうした観点から、本報告書では、対策の情報としてまず運用上の対策を紹介し、そのあとで実装上の対策を紹介している。

4.7. 運用上の対策

4.7.1. 閉じたネットワークの利用

SIP/RTP 関連プロトコルを利用するとき、よく管理されたネットワークを利用できる場合に採用できる対策として、閉じたネットワーク上で SIP/RTP を利用する、という方法がある。閉じたネットワークとは、ネットワークを物理的または論理的に分離または隔離して、SIP/RTP 関連製品を使うネットワークと、それ以外のネットワークを分けて、管理・制御することである。簡単に言えば、閉じたネットワークとは、アクセス制御がきちんと行われ、よく管理された IP ネットワークである、ということである。

例えば Ethernet の VLAN 機能や、802.1X ポート認証機能、無線 LAN の仮想アクセスポイント機能や、マルチ SSID 機能などを利用して、端末認証を成功した端末だけが、特定のネットワークに接続できるように強制することができる。また、広域の VPN サービスで

も認証方法によっては検討候補となる。また、認証ができないような機器が SIP/RTP 関連のネットワークにアクセスするための、Ethernet スイッチの接続ポートやケーブルを物理的に異なる機器に収容して分離・隔離することも検討候補となる。

SIP/RTP 関連プロトコルを利用する上での「閉じたネットワークの利用」で行われる制御の中身は、SIP/RTP とは異なる、IP レイヤや Ethernet レイヤでのアクセス制御である。別の言い方をすれば、SIP/RTP そのものには現在のところ、SIP/RTP の通信内容を暗号化するなどの保護機能が普及していないため、SIP/RTP よりも下の通信レイヤで保護することが「閉じたネットワーク」の意味である。

ただし、一般的に閉じたネットワークは柔軟性に欠ける問題があり、その他の Web サービスや通信サービスとの協調方法に配慮が必要である。また、よく管理された IP ネットワークを利用するには、当然のことながら、よく管理できる人材が必要になる。

4.7.2. IP ネットワークのアクセス区間の保護

閉じたネットワークでは、端末のアクセス制御が行われて、SIP/RTP を利用する端末以外は接続できないようにする。その上で、SIP 端末と SIP サーバの間のネットワーク、すなわちネットワークの「アクセス区間」を保護することで、通信内容の機密性や一貫性が保たれる。

アクセス区間の保護には、例えば無線 LAN では WPA(Wi-Fi Protected Access)認証・暗号化機能を利用したり、外出時のリモートアクセスなどに IPsec や SSL-VPN などの暗号化トンネルプロトコルを利用して、SIP/RTP 関連プロトコルの通信を保護できる。

4.7.3. IP ネットワークのアクセス区間の保護: IPsec

ここでは特に 3GPP IMS(IP Multimedia Subsystem)標準で、2007 年 9 月現在、アクセス区間の保護方法として規定されている IPsec について触れておく。

IPsec での SIP/RTP の保護は、既存の企業向け IP 電話利用者が、外出先から社内の IP 電話システムに接続する場合などに使われている方法でもある。

IMS では、移動端末から見て最初の SIP プロキシサーバである P-CSCF(Proxy-CSCF)までを IPsec の ESP モードで保護する。ESP モードは Encapsulating Security Payload の略で、IP ヘッダを含む RTP のペイロード全体について暗号化とメッセージ署名を行い、機密性と一貫性を保護する。

IMS でのポイントとして、IPsec 中の処理のうちでも特に重い、IPsec 用の鍵交換には、携帯電話の無線接続を行った段階で生成されたマスター鍵を再利用することで、鍵交換の処理を軽減している点がある。IMS の IPsec では、特定のホストと固定的に IPsec 通信を行い、不特定多数のホストとの通信を避けることで、端末側のセキュリティ機能や、SIPS や SRTP などの個別の暗号通信処理機能を不要にしている。

ただし、IMS のようなアプローチは、WPA のような無線 LAN の通信セキュリティ方式から見ると冗長であるし、一般的に IPsec はカーネル内に実装されているために、OS 上での実行権限や設定変更の権限に問題があるなど、アプリケーションから制御しにくい、という問題もある。

4.7.4. ファイアウォール、侵入検知システムの利用

ファイアウォール、侵入防止システム(IPS: Intrusion Prevention System)は、一般的にコストの関係や機能のため、設置できる場所が限定されるが、不正な形式のメッセージや、異常なトラフィック、異常な状態でのリクエストなど、SIP/RTP 関連プロトコルの内容に応じた対応ができる製品も提供されており、検討の可能性がある。SIP/RTP 関連プロトコルを利用する環境で、ファイアウォール、IPS を導入する際は、特に SIP/RTP に対応しており、想定する利用方法に問題がないことを確認する必要がある。

4.7.5. セッション・ボーダー・コントローラの利用

SIP/RTP に対応した製品としてセッション・ボーダー・コントローラ(SBC: Session Border Controller)が広く使用されている。SBC は一般的な SIP エンティティとして機能するため、SIP/RTP 関連プロトコルの内容に応じた処理を行うことが可能である。

SBC が提供する機能として、アドレスの書き換えによるトポロジの隠蔽、SIP メッセージの内容に応じたアクセスコントロールがある。また、トラフィック制御による DoS 攻撃がからの防御、不正メッセージの中継拒否といった機能により内部のネットワーク機器を防護することが可能である。

SBC の機能についての情報は、RFC5853(*1)にまとめられている。

4.8. 実装上の対策 – SIP 関連プロトコルの保護対策

4.8.1. SIP での TLS 利用について

SIP は、「4.7.1 閉じたネットワークの利用」で紹介したように、インターネットや一般のネットワークユーザから隔離したネットワークで利用することで、安全を確保することもできる。しかし、SIP を利用した製品が普及するにつれて、よりオープンなネットワークで利用される場合も増えている。例えばインターネットや、管理が行き届かないネットワークでも SIP 関連プロトコルを安全に利用するために、SIP 関連プロトコルそのものを暗号化する機能を利用できる。

本報告書執筆時点では、SIP そのものに関しては TLS(Transport Layer Security)が、RTP そのものに関しては SRTP(Secure RTP)が標準化されている。TLS と SRTP に対応した製品はまだ豊富とは言えないが、着実に増加しており、今後、SIP 関連プロトコルを利用する製品に対応が求められると見られる。

ただし、TLS と SRTP についてはまだ他の方法が提案されている状況もあり、開発途上の部分も見られる。ここでは SIP を保護する TLS について、新しく提案されている方式も参考として整理しておく。なお、SRTP については「項目 8 - RTP メディアの盗聴から起こる問題」を参照していただきたい。

1) SIP over TLS over TCP
SIP プロトコルの標準仕様 RFC3261(*2)で標準化されている SIP の保護方法。
TCP 上でソケットインターフェースを利用して保護機能を提供する TLS を使う。

2) DTLS-SRTP Framework
SIP の保護とは独立して、RTP の保護を SRTP で行う提案。SRTP 用の鍵は UDP 上の TLS である DTLS(RFC4347 Datagram TLS*3)を利用する。RFC5763(*4)で標準化されている。

IPsec や SSL-VPN については、SIP/RTP のレイヤよりもひとつ下のレイヤで処理される

[1] RFC5853: Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments (http://tools.ietf.org/html/rfc5853)
[2] RFC3261 SIP, 26.4.3 TLS (http://tools.ietf.org/html/rfc3261#section-26.4.3)
[3] DTLS は OpenSSL 0.9.8 以降でサポートされている (http://openssl.org)
[4] RFC5763: Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layser Security (DTLS)
(http://tools.ietf.org/html/rfc5763)

方法のため、実装上の対策としては触れていない。ただし、3GPP の IMS 標準のように、IPsec が標準的な SIP/RTP の保護方法である、とする仕様もあるのでご注意いただきたい。

4.8.2. TLS 利用上の注意点

SIP/RTP とともに TLS または DTLS を利用する場合、さまざまな利用方法が想定されるが、一般的に SIP 環境での TLS の利用にはいくつかの注意が必要である。

1) まず、SIP での TLS は SIP 端末と SIP サーバの間で、ポイントツーポイントで利用され、SIP 端末と SIP 端末の間でエンドツーエンドでは利用されない。
2) TLS 接続を開始するときには、一般には TLS セッションを受け入れる、SIP サーバ側が、サーバのホスト名や IP アドレスを証明するサーバ証明書を用意する必要がある。
3) 実際に TLS 接続を行うときには、SIP 端末は SIP サーバから提示されたサーバ証明書を、信頼する第三者である、ルート証明書で「検証」しなければならない。
4) その後、公開鍵暗号を利用して安全に鍵交換を行うが、この処理の負荷に注意が必要である。

4.9. 実装上の対策 - ソフトウェア開発共通の課題

4.9.1. 脆弱性報告の大半を占める「不具合を起こしやすいパケットに対応できない問題」

12 番「不具合を起こしやすいパケットに対応できない問題」で指摘されている理由で、実際に不具合を起こす製品は多数存在し、脆弱性情報データベースなどに報告されるほとんどの脆弱性が、12 番の脆弱性に該当する。ここでは、「不具合を起こしやすいパケットの問題」に関して指摘されている、ソフトウェア開発に共通する問題点と注意事項を整理しておく。なお、ここでいうソフトウェア開発は、製品やサービスの企画を含む、設計、コーディング、テストから、機器のマニュアルや付属品を含むパッケージング、発送までの広い意味での製品提供者側の作業のことを指す。

SIP 関連のセキュリティ製品を開発、販売する Sipera 社は、独自に収集した脆弱性情報を分析したところ、20,065 件の脆弱性のうち、20,000 件以上が SIP サーバ製品に対する不正な形式のメッセージを含むパケットによる不具合だった、と発表している(Comprehensive VoIP Security for the Enterprise)。

現在も、CVE(Common Vulnerabilities Exposures)や JVN(日本脆弱性レポート)などの脆弱性データベースに掲載される脆弱性報告の多数に、「バッファオーバフロー」「ヒープオーバーフロー」が原因として指摘されている。この両者だけでも 2007 年 8 月 1 日～9 月 24 日までの JVN の脆弱性情報 100 件のうち、31 件がバッファオーバフローかヒープオーバーフローであった。特に最近は OS や著名なソフトウェアだけではなく、一般のシェアウェアを狙った攻撃が増えているのが特徴である。今後、SIP 関連プロトコルを利用した機器に対しても、不正な形式のメッセージによる、機器ののっとりを狙った攻撃が行われるようになるのは時間の問題とも言われている。

ただし、裏を返せば、不正な形式のメッセージによる問題はすべてのコンピュータソフトウェアに共通の問題であって、SIP 関連製品に特有の問題ではないことにも注目したい。SIP 関連以外でも、不正な形式のメッセージに対応するために、ソフトウェアのコーディング段階や製品化後に、自動的にテストや検査を行うツールがいくつかあるので、こうしたツールを利用することができる。

また、製品内に Web サーバを搭載する場合の問題や、外部の Web サーバなど、他のアプリケーションと連携する際の問題については、Web アプリケーションの開発ガイドや「Web アプリケーションセキュリティ」などの対策情報が公開されているので、検討ができる。

残る問題は、SIP や RTP の正しい形式のメッセージでも、不具合を起こしやすいメッセ

ージが存在する点である。これにてついては攻撃手法と対策方法の双方とも、情報が不足しているため、さらなる研究開発が必要な分野と考えられる。

4.9.2. ソフトウェア開発中の根本的な対策 - 利用方法の特定と脅威の特定

セキュリティの基本であるが、コンピュータソフトウェアを開発する際のステップを踏んでおくことがまずは重要である。その第一として、利用方法の特定である。ある SIP/RTP 対応機器を開発するときに、その機器がどのような場面でどのような人が、どのような手順で何に利用するのか、ということを明確にすることである。例えば、オープンなネットワーク環境で利用するのか、それとも IP 電話専用のネットワークなどで利用するのかによって、機器に求められる安全性や耐性は大きく変わる。また、機能が多ければ、例外事項も増え、テスト項目も増加する。利用者のスキルやトレーニングをあてにするかどうかも安全性に大きく関係する。所定のマニュアルどおりに操作する専用機器と、一般消費者が利用する家電並みの機器とでは、想定外の利用に対する対応方法も異なる。

こうした利用条件を特定できれば、脅威の範囲も明確になり、テストの対象範囲やテストの詳細度も特定しやすくなる。脅威の分類と優先度付けを行うことで、脅威への対応コストを最適化する手法については「脅威モデル」で展開されている。

ただし、利用方法の特定と脅威の特定は、一般的には時間がかかる。特に汎用的な機器になるほど、利用方法は多岐にわたるため、脅威を体系的に整理しなければならないなどの手間がかかると考えられ、製品によって得られる利益と、体系的に整理するためのコストのバランスを検討する必要がある。

4.9.3. 企画・設計時の対策

企画、設計段階では、認証手順を含む利用手順そのものや、機器が備えるインターフェースや機能、その他の外部機器やサービスとの通信方法などの外部インターフェース、提供するサービス品質などが、脆弱性対策に関係する。

Web アプリケーションで問題になる、ユーザや端末からのリクエストの内容の正規化(sanitization: 消毒)、ディレクトリトラバーサルや、クロスサイトスクリプティングの回避などは、コーディングに入る前の、関数やプログラムの具体化方法を決める、詳細設計時点までには対策を盛り込んでおく必要がある。理想的には外部インターフェース設計をする時点で、セキュリティ対策として検討しておくとよい。

ただし、企画設計時点でのセキュリティ対策は一般的には、利用する技術の専門的な知識が必要であることが多いため、対策を保障するライブラリやミドルウェアを利用したり、必要とする技術要素の分野のトレーニングを受けることも有効である。

4.9.4. コーディングレベルでの検査の自動化とその他の対策

コーディング時に注意すべき問題と対策が、特に C 言語または C++言語について、まとめられている。「IPA ソフトウェア開発者向けのページ、1. セキュリティ脆弱性の低減」では、基本的な注意点が Web にまとめられている。また、「C/C++セキュアコーディング」(歌代 和正 監訳、JPCERT/CC 訳、ASCII、2006 年)では、コーディング時に混入する脆弱性の詳細な説明のほか、自動的にソースコードを検査して、脆弱性を排除するために自動的にソースコードを検査する製品の紹介もある。

また、Visual C++ 2010 などの最新の開発環境にも、コーディング時の脆弱性を回避するための警告機能がある。オープンソースのコンパイラである GCC (GNU C Compiler)の最新版にも、スタック上のコード実行を抑止する機能や、スタックオーバーフローなどへの対策機能がある。また、脆弱性を含む関数が排除されたライブラリや、メモリの破壊をしにくくするライブラリなども提供されており、利用を検討することができる。

さらに目を転じて、C/C++言語ではなく Java のような安全に実行することを前提に作ら

れた言語を利用する方法もある。C/C++言語は、メモリを直接扱うことができ、柔軟で高速なプログラミングが可能だが、同時に脆弱性をはらむ危険も大きい。しかし、メモリ上のデータが抽象化され、アドレスやポインタを直接操作することがない、Java や.NET(ドットネット)のようなバイトコンパイル型の言語は C/C++言語よりも安全にコーディングしやすい。一般にバイトコンパイル型の言語は、それを処理するための仮想マシン(VM)のために、CPU 能力やメモリ容量の追加を要するデメリットや、既存の C/C++ソースコードを書き直す手間などのデメリットがあるが、サーバ機器や高機能端末のように、条件が合えば検討が可能だろう。

4.9.5. 製品化後の検査

不正形式データを送る検証ツールがいくつか存在するので、製品化が済んだあとで脆弱性を検査するのに利用できる。このカテゴリの製品のキーワードとしては”Fuzzing”や、”Tolerance”などがある。代表的なテスト製品の例としては PROTOS Test Suite(c07-sip)の後継製品などがある。いくつかのプロトコルごとに、不具合の発生が想定される、あるいは実際に不具合が発生した事例を元に数万以上の、不具合を誘発するメッセージを送信して、対象製品の脆弱性を検査できる。

製品化後の検査は、検査環境の構築や、数万点の検査結果の評価を行った後、開発ステップに戻って修正を行い、製品ソフトを再配布する、などの対応が必要になり、多くのコストがかかる。製品化されてしまった機器については、製品化後のテストを行う製品が有用だが、企画・開発段階にある製品は、できるだけ早い段階で検証を行うのが理想である。

4.9.6. ハイレベルのプロトコルスタックの脆弱性対策

SIP や RTP の仕様に準拠しつつ、例外条件や想定外動作をテストするツールは市販品は改良が進み、Codenomicon 社やネクストジェン社の SIP 脆弱性スキャナは RFC4475 の「SIP 拷問テスト」のテストパターンや複数の手順を組み合わせたパターンが含まれている。これらの試験ツールは数万～数百万の試験シナリオを具備しており、これらのシナリオを死活監視を行いながら順次実施する機能を具備している。

4.9.7. 他の機能と連携するときの脆弱性

SIP/RTP 関連の処理機能とは別の、Web サーバ機能を呼び出したり、SQL データベース機能を呼び出したりするときに、不適切なコマンドやリクエストを渡すと、予期しない動作が引き起こされることがある。このような外部アプリケーションと連携するときに起こりやすい不具合、脆弱性については、「Web アプリケーション脆弱性」などのキーワードで整理されている（IPA セキュア・プログラミング講座)。

4.9.8. SIP/RTP を利用した製品のテスト方法

一般にソフトウェアやハードウェアの開発段階では、仮想のエンドユーザが期待どおりに利用手順を進められるシナリオを「正常系」、そうではない例外が発生したり手順が中断、失敗、やりなおしになるシナリオを「異常系」などと呼び、それぞれについて試験を行われている。本報告書にまとめられている、標準仕様以外のメッセージや、予期していなかったメッセージへの対応はほとんどが異常系のテストとして実行されるべきものである。

しかし、SIP/RTP はプロトコル仕様が柔軟な反面、さまざまな内容のメッセージが交換される想定が可能で、完全なテストを行うためには非常に多数の試験項目が必要となってしまう。特にテキストで表現された SIP プロトコルでは、例えば「4 オクテットの符号つき数値」を表現する行であっても、実際のワイヤ上を転送されるデータとしては数千文字のテキストを並べることもできてしまう。

一方で、IPv4 や TCP の場合はヘッダフィールドが固定長のビット列であり、SIP のような自由度はなく、SIP に比べればテストは行いやすい。そのため、SIP/RTP を利用した製品のテストには、TCP/IP レベルのテスト方法とは違ったアプローチを検討する必要があるだろう。特に、多数のメッセージ形式や、プロトコルの状態、複数の値や表現方法に対応できるような、自動化された、多数のテストパターンの生成が求められている。

4.9.9. 脆弱性を排除するテストを実施するには？

しかし、一般的にネットワーク機器や情報家電製品は、ソフトウェアによる提供機能が横並びになるにつれ、低価格かどうかが最大の選択ポイントになっており、個別の情報家電機器のテストが行われなくなっているのが実情である。また、市場や流通現場からは、機能を提供する早さが求められており、AJAX や Web 2.0 のようなキーワードは「テストよりも機能提供を先に」という姿勢を含んでいる、という問題点も指摘されている。

本来は脆弱性を持たないように作られた製品が出荷されるべきであるが、利用者には脆弱性がわからないまま、問題がある製品が流通してしまっているのが現状である。こうした中で、脆弱性を持たない製品を出荷させるようにする仕組みはどのようなものが必要なのか、検討する必要がある。

例えば、ROHS 指令のように、有害物質を含む製品を排除する国際規制のように、ソフトウェアの脆弱性についても規制が行われることは時間の問題であると考えられる。また、直接的な規制ではないが、ボットに感染したパソコン利用者はインターネット接続させないよう、ISP(インターネットサービスプロバイダ)が規制できるようにする、という業界の対応も、間接的ながら、脆弱性を含む製品を排除する後押しになると考えられる。

また、ソフトウェア一般の共通原則として、ソフトウェアの不具合は完全にゼロにできない、という問題がある。この前提に立つとすれば、情報機器はソフトウェアを随時適切に更新することで、そのときどきの脆弱性を数ヶ月以内に解消する、などの善後策も必要である。

最悪の事態は、2007 年夏のアメリカで起きているような、鉛を含む玩具やベビー用品を出荷したあとで、百万台にもおよぶ製品回収に至る事態である。このように大量に製品が出荷されたあとでは、たとえ販売会社が回収作業を行ったとしても、現実的には製品回収は難しく、被害が発生するのを待つだけになってしまう。

5. 脆弱性項目解説

本章では、SIP に係わる代表的な既知の脆弱性について、概要、解説、対策、その他参考情報について記述を行う。

【 項目 1. SIP リクエストの偽装から起こる問題 】

項目1. SIP リクエストの偽装から起こる問題

1.1 概要

SIP のリクエストを盗聴し、リクエストを偽装することにより、正規のシーケンスの妨害や、不正なセッションの確立を行える可能性がある。

図 1-1 は、攻撃者の SIP 端末が発信側の SIP リクエストを盗聴することによって、必要な情報を獲得し、偽装された SIP リクエストを送信している例である。

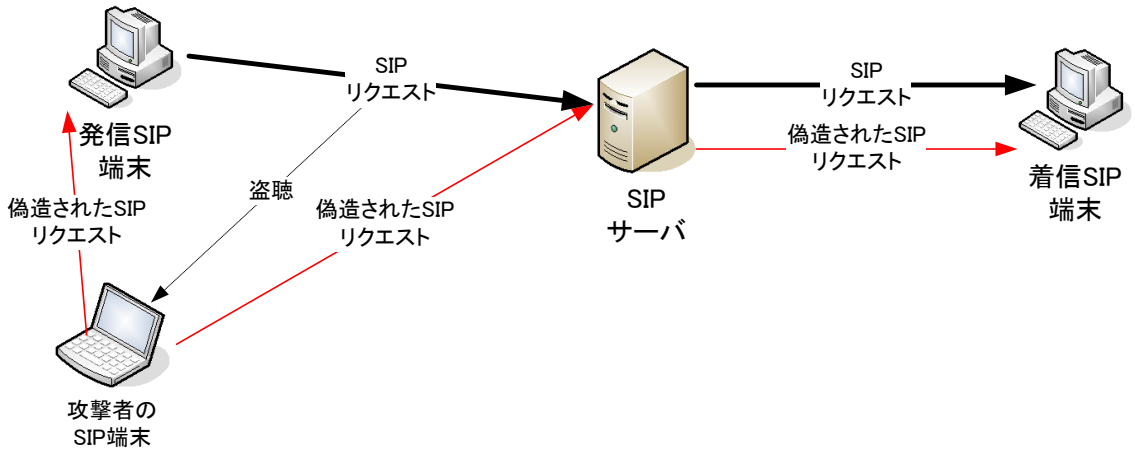


図 1-1 盗聴と偽装

なお、この節では、SIP リクエストに対する認証については以下のような仮定をとる。

1) リクエストに対して認証が要求されない
2) 認証に必要なパスワードが盗まれている
3) 後述の「SIP 認証パスワードの解読」「認証機能の不十分な実装の問題」で指摘されているような手法により、認証が無力化されている

解説の図中では、上述 1) の場合を仮定して説明を行っている。

1.2 解説

【攻撃手法とその影響】

偽装されたリクエストには以下のような種類がある。

1) REGISTER リクエストの偽装
2) CANCEL リクエストの偽装
3) re-INVITE リクエストの偽装
4) BYE リクエストの偽装
5) PRACK リクエストの偽装

メッセージの種類によって、攻撃により受ける影響は変わってくる。

【 項目 1. SIP リクエストの偽装から起こる問題 】

1) REGISTER リクエストの偽装

SIP 端末が INVITE リクエストなどの SIP リクエストを受信するために、自身の IP アドレスとポートを、SIP サーバに登録ために使われるのが REGISTER というリクエストである。

既に REGISTER リクエストによって登録されている、SIP 端末の情報(IP アドレス等)に対して、第三者からの偽装された REGISTER リクエスト送信によって以下の行為が可能となる。

① 登録削除により着信させない
② 登録書き換えによる着信の横取り

図 1-2 は、SIP 端末が登録のために SIP サーバに送信した REGISTER リクエストのパケットを、攻撃者の SIP 端末が盗聴している状況を表している。

攻撃者による盗聴によって、REGISTER リクエスト内で使用される Call-ID などの情報が分かると、攻撃者の SIP 端末は「登録削除」や「登録書き換え」の偽装 REGISTER リクエストを送信できるようになる。

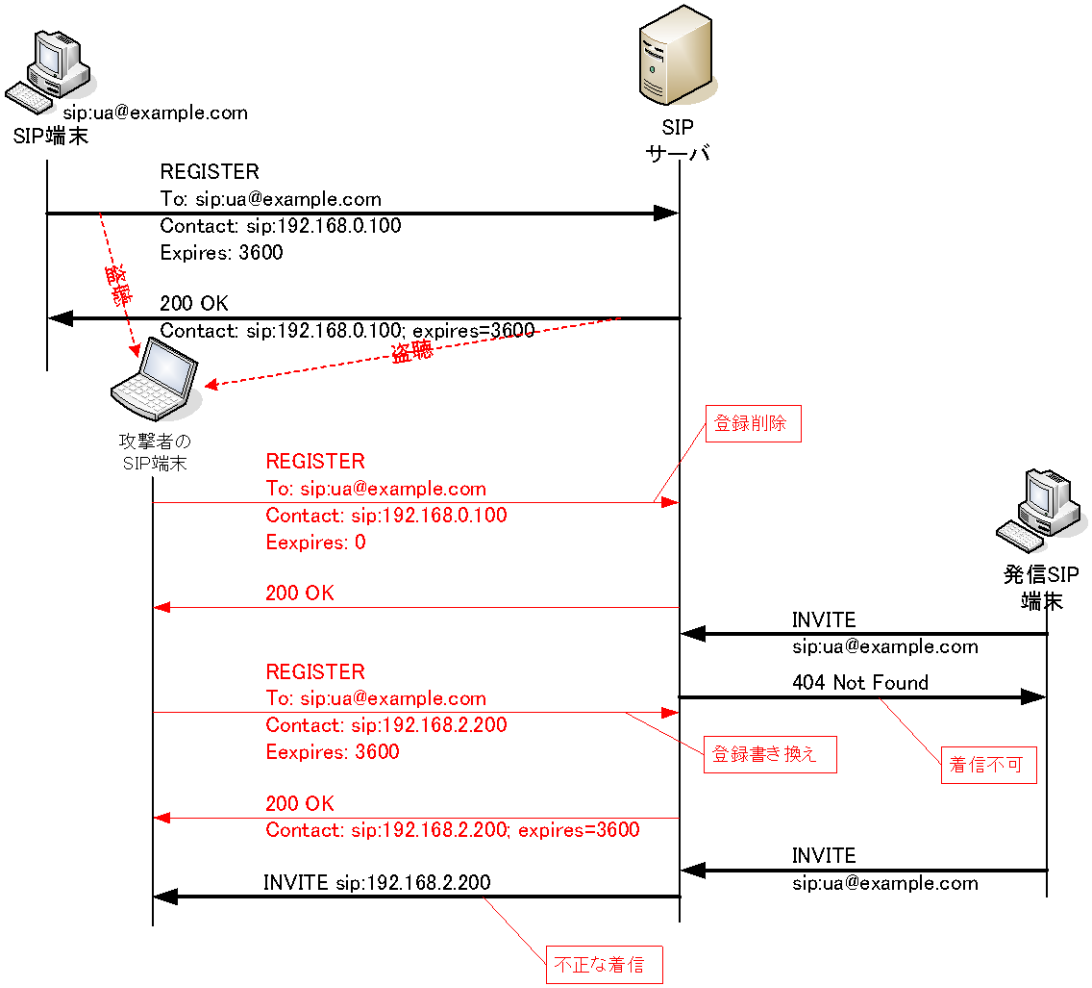


図 1-2 登録の削除と登録の書き換えのシーケンス

【 項目 1. SIP リクエストの偽装から起こる問題 】

「登録削除」の偽装 REGISTER リクエストによって、SIP サーバの登録情報が削除された状態では、SIP 発信端末から SIP 端末[sip:ua@example.com]宛の INVITE リクエストが SIP サーバ受信されても 404 レスポンスで拒否されてしまう。

また、「登録書き換え」の偽装 REGISTER リクエストが、攻撃者の SIP 端末の IP アドレスで SIP サーバ上の登録情報を書き換えてしまった状態で、SIP 発信端末から SIP 端末[sip:ua@example.com]宛の INVITE リクエストが SIP サーバ受信されると、INVITE リクエストが攻撃者の SIP 端末に着信してしまい、通話を横取りされる。

2) CANCEL リクエストの偽装

INVITE リクエストに対して、ダイジェスト認証などを用いてユーザを認証したとしても、悪意のある第 3 者が CANCEL リクエストを偽装して送信した場合、発信 SIP 端末のユーザの意図にかかわらず発信が取り消されてしまう可能性がある。

図 1-3 は攻撃者の SIP 端末が INVITE リクエストを盗聴し、Call-ID などの必要な情報を取得することによって、偽装された CANCEL リクエストを送信し、発信を取り消している状態を示している。CANCEL リクエストを送信するタイミングは 100 Trying レスポンスが着信 SIP 端末から送信された後でなければならないので、CANCEL リクエスト送信のタイミングのために 100 Trying レスポンスも盗聴する必要がある。偽装された CANCEL リクエストを受信した着信側 SIP 端末は 487 Request Terminated レスポンスを送信し、着信側 SIP 端末は発信が拒否されたと判断してしまう。

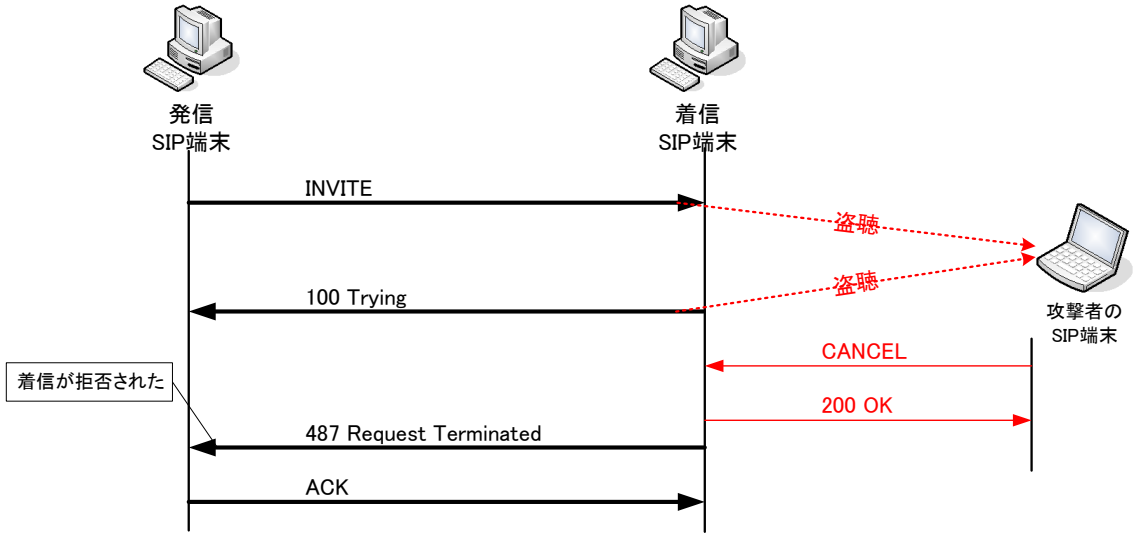


図 1-3 偽装された CANCEL リクエストのシーケンス

RFC3261 の 22.1 Framework では、CANCEL リクエストを受け取った SIP サーバが、取り消しの対象となる INVITE リクエストと同じ経路で CANCEL リクエストが送信されていることを確認するように求められている。そのために、トランスポートレイヤーまたはネットワークレイヤーで送信元となる SIP 端末(またはサーバ)を確認するという前提が記述されている(ただし、具体的な確認手段に関する記述は無い)。

一般的な SIP の実装では主に UDP が使用されているので、INVITE リクエストをネットワーク上でキャプチャできれば、IP アドレスを含めて、偽装された CANCEL リクエストは、容易に作成できる。

【 項目 1. SIP リクエストの偽装から起こる問題 】

3) re-INVITE リクエストの偽装

re-INVITE リクエストとは、確立したダイアログ内で送信される INVITE リクエストのことであり、セッション確立の確認や、メディア情報(コーデックの種類、メディア送信の保留・保留解除)の変更のために使用される。

INVITE リクエストにより正常に通話などのセッションが確立された後、偽装された re-INVITE リクエストによって既存のセッションが乗っ取られる場合がある。

図 1-4 は通話が成立した後で、攻撃者の SIP 端末から偽装された re-INVITE リクエストが送信されている状況を示している。まず、発信 SIP 端末から INVITE リクエストが送信され着信側 SIP 端末との間にセッションが確立し音声による通信が行われている。このときに送受信された正規の SIP リクエストとレスポンスが、攻撃者の SIP 端末に盗聴された場合、盗聴者の SIP 端末は着信 SIP 端末には偽装した BYE リクエストを送信してセッションが切断されたように見せかけ、発信 SIP 端末には re-INVITE リクエストを送信しセッションを乗っ取ろうとしている。この偽装された re-INVITE リクエストの Contact ヘッダや SDP 内には、攻撃者の SIP 端末の IP アドレスが記述されており、発信 SIP 端末は攻撃者の SIP 端末と通和状態になってしまう。

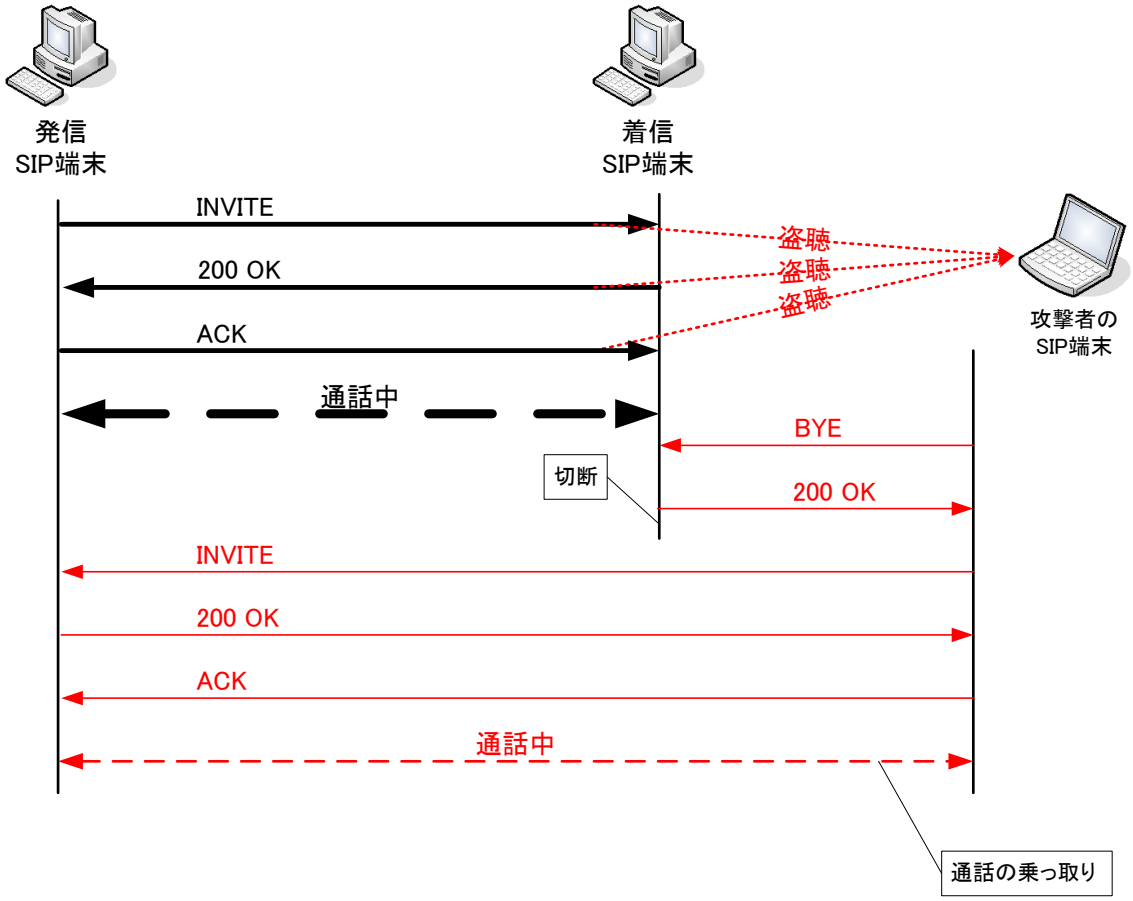


図 1-4 偽装された re-INVITE リクエストのシーケンス

【 項目 1. SIP リクエストの偽装から起こる問題 】

4) BYE リクエストの偽装

INVITE リクエストにより正常に通話などのセッションが確立された後、偽装された BYE リクエストによって既存のセッションが切断され、その結果、通話が意図せず切断される場合がある。

図 1-5 の例では INVITE リクエストなどを盗聴し必要な情報を取得した攻撃者の SIP 端末が、偽装した BYE リクエストを発信 SIP 端末と着信 SIP 端末に送信することにより通話を切断している状況を表している。まず、発信 SIP 端末から INVITE リクエストが送信され着信側 SIP 端末との間にセッションが確立し音声による通信が行われている。このときに送受信された正規の SIP リクエストとレスポンスが、攻撃者の SIP 端末に盗聴された場合、盗聴者の SIP 端末は発信 SIP 端末と着信 SIP 端末の両方にそれぞれ偽装した BYE リクエストを送信してセッションが切断されたように見せかけ、通話が切断されてしまう。

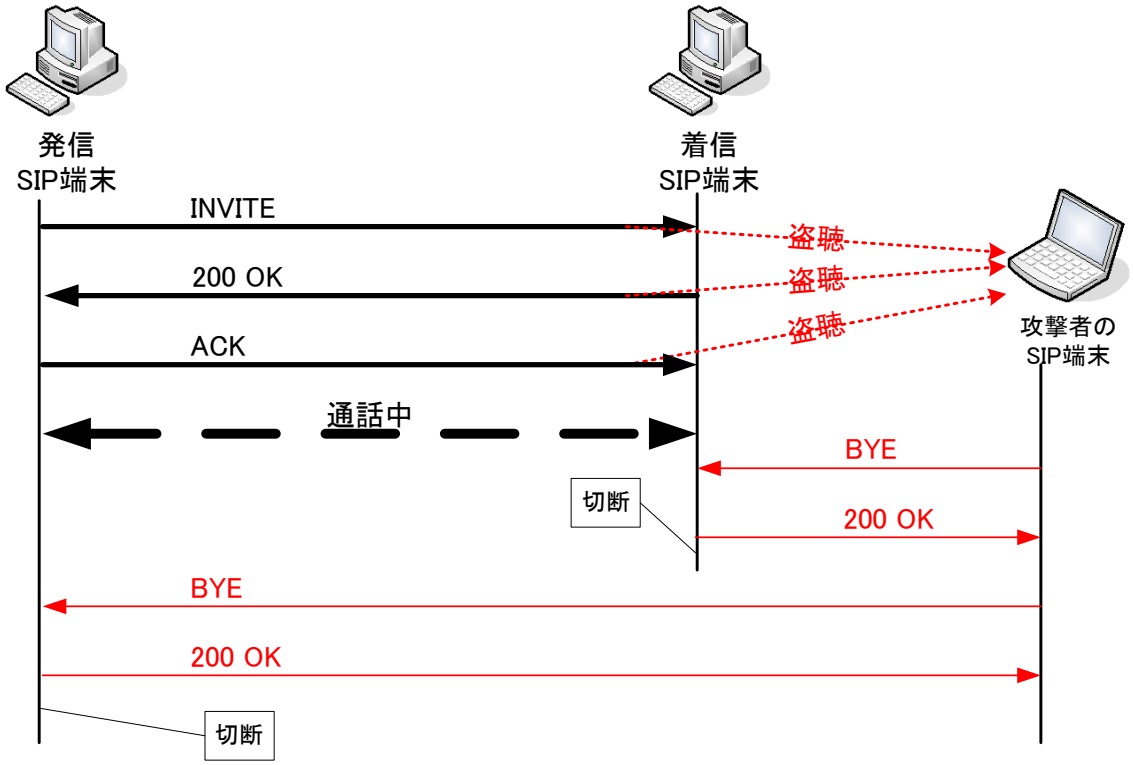


図 1-5 偽装された BYE リクエストのシーケンス

【 項目 1. SIP リクエストの偽装から起こる問題 】

5) PRACK リクエストの偽装

SIP のリクエストやレスポンスは UDP で送られる場合がある。UDP はその仕様の範囲内では、送信パケットの受信を、送信側が確認できない。受信の確認が必要な場合は、受信側から確認のためのパケットを別途送信する必要がある。SIP でも、ACK 以外のリクエストに対してはレスポンスを送信することが定められている。だが、レスポンスの受信をレスポンスの送信元が確認しなければならない場合があり、具体的には INVITE リクエストの最終応答と信頼性の必要な暫定応答である。ここで言う信頼性とは、パケットの受信状態に関して、送信側と受信側の認識を同期できるという意味であり、具体的には受信確認のリクエストが正しく送受信された状態を指す。INVITE リクエストの最終応答の受信確認に使われるのが ACK リクエストで、信頼性の必要な暫定応答の受信確認に使われるのが PRACK リクエストである。

この PRACK リクエストが偽装された場合、暫定応答の信頼性が損なわれてしまう可能性がある。

図 1-6 の状態で、着信 SIP 端末は受信した INVITE リクエストに対して 183 Session Progress レスポンスを送信している。

攻撃者の SIP 端末はこの 183 Session Progress レスポンスの送信を盗聴した直後に、偽装した PRACK リクエストを送信している。このことにより受信 SIP 端末は、発信 SIP 端末が 183 Session Progress レスポンスを受信したと判断するが、実際には発信 SIP 端末の送信した正規の PRACK リクエストは遅れて受信 SIP 端末に届き、500 Server Internal Error で拒否される。この時点(図中の①)で発信 SIP 端末は 183 Session Progress レスポンスの受信を受信し、SIP 端末の確認が出来ていないと判断する。この状態で、新たな 180 Ringing レスポンスが送信されても、発信 SIP 端末は新しい暫定応答(180 Ringing)の確認処理(PRACK 送信)に移行できない可能性が高い。その結果、着信 SIP 端末では 180 Ringing レスポンスの再送が起こり、結局 180Ringing レスポンスの信頼性は確認されない。また、偽装された PRACK リクエストに SDP が記述されていた場合は、トーン信号の入力を促す通話前アナウンス等が横取りされる可能性もある。

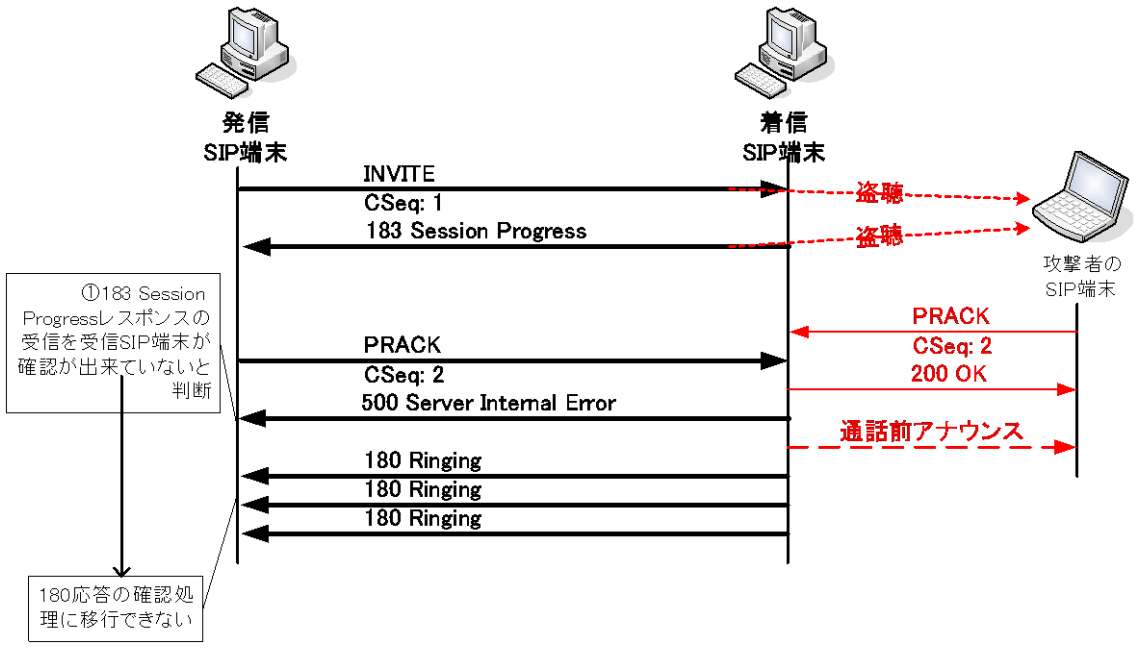


図 1-6 偽装された PRACK リクエストのシーケンス

【 項目 1. SIP リクエストの偽装から起こる問題 】

【原因と考察】

偽装した SIP リクエストによる攻撃は、正規の SIP リクエストとレスポンスが盗聴されていたり、SIP 認証が効力を失っている場合に成功する確率が高い。SIP 認証が効力失っている場合とは以下のような場合が考えられる。

1) SIP リクエストに対して SIP 認証が要求されない
2) SIP 認証に必要なパスワードが盗まれている
3) 後述の「SIP 認証パスワードの解読」「認証機能の不十分な実装の問題」で指摘されているような手法により、SIP 認証が無力化されている

なお、以下に CANCEL リクエストで SIP 認証を要求できない理由を説明する。

CANCEL リクエストに関しては、認証要求の SIP レスポンス(401/407)による再送信ができないため、認証の手法が使えない。これは、再送信する際には通常 CSeq ヘッダの値を 1 増加させるのだが、CANCEL リクエストの CSeq 値は取り消す INVITE リクエストと関連付けるため、INVITE リクエストの CSeq 値と同じにしなければならないという特殊な制約があるからである。例えば、CSeq 値が 1 の INVITE リクエストを取り消すための CANCEL リクエストは CSeq 値が 1 で無ければならない。この CANCEL リクエストが 401 Unauthorized レスポンスで認証を求められると CSeq 値を 1 増加させて CANCEL リクエストを再送信することになるが、取り消したい INVITE リクエストの CSeq 値は 1 のため、対応が取れなくなる。

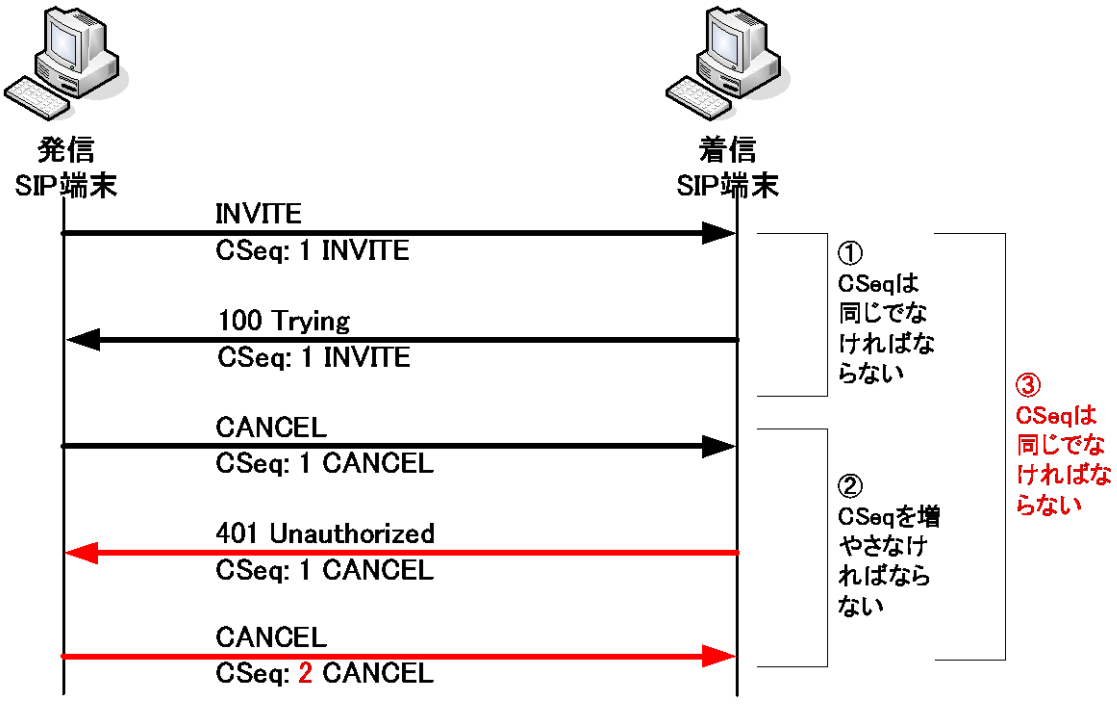


図 1-7　CANCEL の Cseq ヘッダ

【 項目 1. SIP リクエストの偽装から起こる問題 】

1.3 対策

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【実装ガイド】

1) S/MIME により End-to-End の暗号化を行う
CANCEL 以外のリクエストは、発信 UA と着信 UA の間(end-to-end)で処理されるので、S/MIME などの暗号化による保護の対象となりうるが、CANCEL リクエストは UA とプロキシサーバの間で hop-by-hop に処理されるため、S/MIME などの暗号化は適さない。

2) Secure SIP (SIP over TLS)の実装

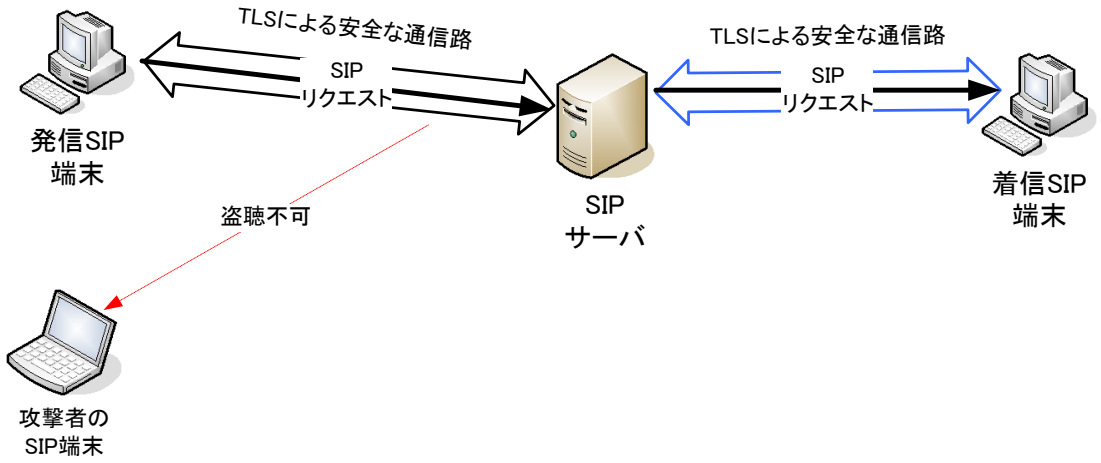


図 1-8 TLS を使った安全な通信路による盗聴の防止

【 項目 1. SIP リクエストの偽装から起こる問題 】

1.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol 10 Registrations http://tools.ietf.org/html/rfc3261#section-10 13 Initiating a Session http://tools.ietf.org/html/rfc3261#section-13 14 Modifying an Existing Session http://tools.ietf.org/html/rfc3261#section-14 15 Terminating a Session http://tools.ietf.org/html/rfc3261#section-15 22.1 Framework http://tools.ietf.org/html/rfc3261#section-22.1
2002 年 6 月	RFC3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP) http://tools.ietf.org/html/rfc3262

1.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	□ Ⅰ （注意）	■ Ⅱ （警告）	□Ⅲ （危険）
本脆弱性の CVSS 基本値		4.0	

※本評価は、深刻度の最も高い「REGISTER リクエストに関する脆弱性」を対象としたものである

【CVSS 基本値の評価内容】(REGISTER リクエストの偽造)

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	■なし	□部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

【 項目 2. SIP レスポンスの偽装から起こる問題 】

項目2. SIP レスポンスの偽装から起こる問題

2.1 概要

SIP サーバになりすまして、SIP リクエストに対する SIP レスポンスを偽装することにより、不正な操作を行う。200 番台のレスポンスを偽装した場合、本来通信するはずのない相手との通信に誘導される。400 以上のレスポンスを偽装した場合、通信が失敗したと発信側に誤解させる。300 番台のレスポンスを偽装した場合は、不正な通信先へ誘導指される恐れがある。

図 2-1 は、攻撃者の SIP 端末が発信側の SIP リクエストを盗聴することによって、必要な情報を獲得し、偽装された SIP レスポンスを送信している例である。

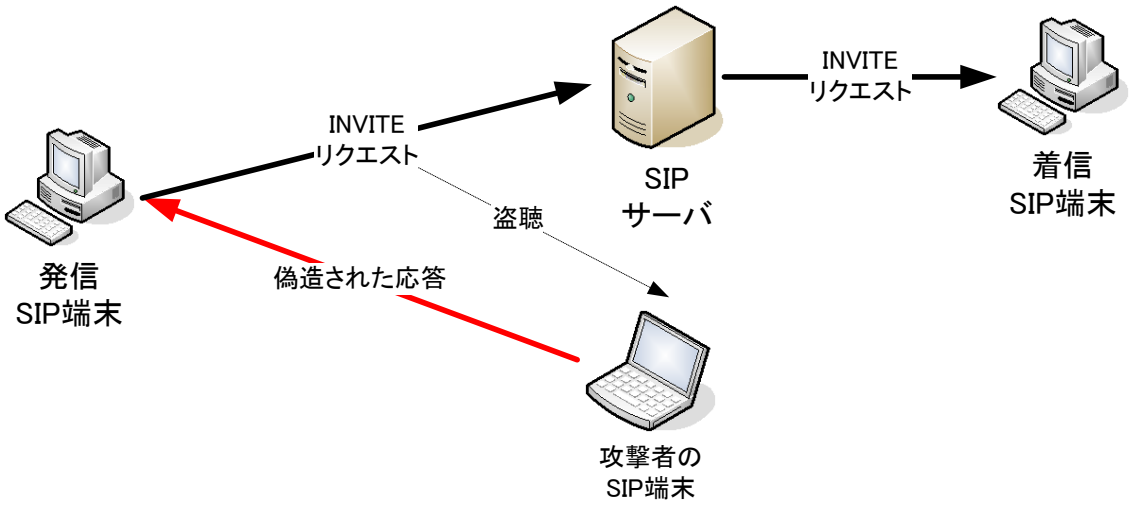


図 2-1 レスポンスの偽装

2.2 解説

【攻撃手法とその影響】

この攻撃手法は、レスポンスの種類によって多くのバリエーションが考えられる。
この節では、以下の 3 つのレスポンスを例にその影響を説明している。

1) 200 OK レスポンス(通信応諾)の偽装
2) 302 Moved Temporarily レスポンス(一時的移動による着信転送)の偽装
3) 404 Not Found レスポンス(宛先不明)の偽装

1) 200 OK レスポンス(通信応諾)の偽装

本項では、INVITE リクエストに対する 200 OK レスポンスの偽装について説明する。
INVITE リクエストに対する 200 OK レスポンスは、着信側の端末が通信に同意したことを意味するレスポンスであり、電話機の操作におけるオフフック(受話器を取り上げること)にあ

たる。

また、200 OK レスポンスには通常 SDP と呼ばれるボディ部が存在し、音声やビデオなどのメディアを送受信するために必要な情報(コーデック、IP アドレスやポートなど)が記述されている。200 OK レスポンスが偽装された場合、以降の SIP シグナリングとメディアの送受信が乗っ取られる。意図しない相手と通信させられることになる。

図 2-2 は、発信 SIP 端末からの INVITE リクエストと、着信 SIP 端末からの 100 Trying レスポンスを攻撃者の SIP 端末が盗聴している状態を示している。攻撃者の SIP 端末は盗聴から得た情報を元に偽装した 200 OK レスポンスを発信 SIP 端末に送信し、着信 SIP 端末になりすます。同時に着信 SIP 端末には偽装した CANCEL リクエストを送信し、発信が取り消されたように見せかけている。

※ ボディ部の SDP を偽装する点については、「項目 4 - SIP メッセージボディの改ざんから起こる問題」を参照

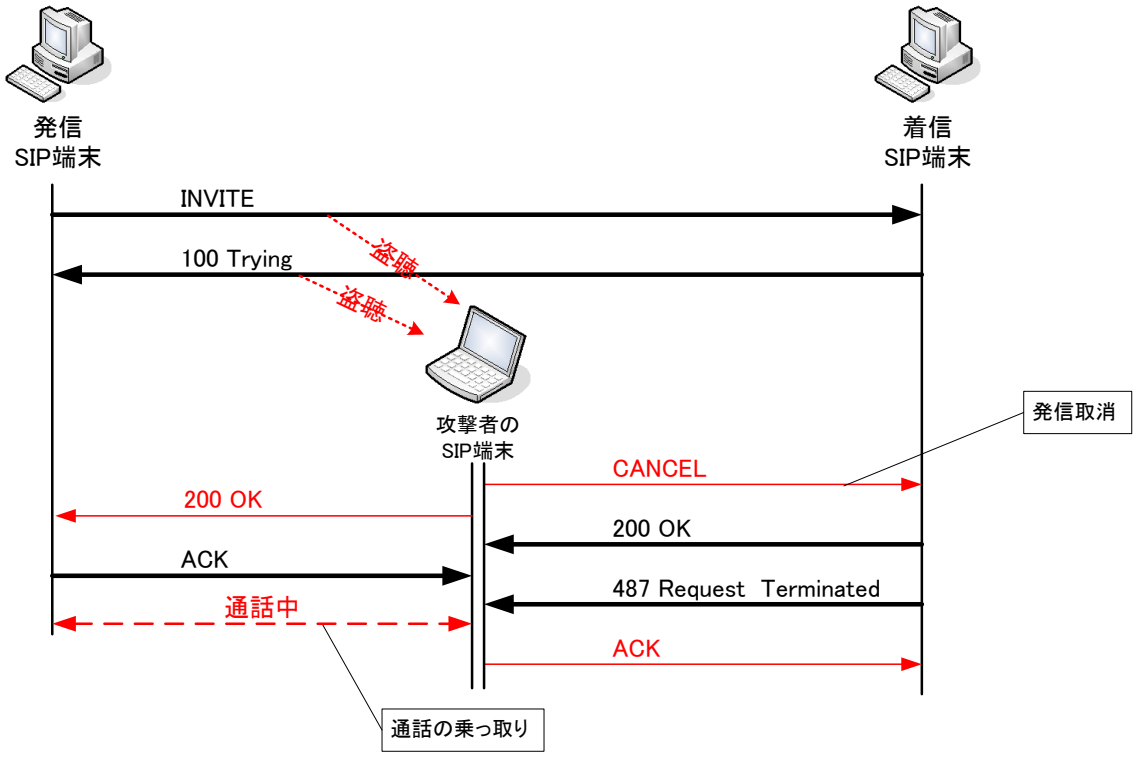


図 2-2 200 OK レスポンス(通信応諾)の偽装

2) 302 Moved Temporarily レスポンス(一時的移動による着信転送)の偽装

本項では、INVITE リクエストに対する 302 Moved Temporarily レスポンスの偽装について説明する。

INVITE リクエストに対する 302 Moved Temporarily レスポンスは、着信側のユーザが一時的に違う端末を使用する状態にあることを意味するレスポンスである。例えば、一時的に別室で作業中なので、その部屋で電話を取りたいような状況が考えられる。移動先の端末を示す新たな SIP-URI は 302 Moved Temporarily レスポンス の Contact ヘッダに記述され、発信側に新たな宛先への INVITE リクエスト送信を促す。

302 Moved Temporarily レスポンスが偽装された場合、発信者の意図しない着信先と通信させられることになる。

【 項目 2. SIP レスポンスの偽装から起こる問題 】

図 2-3 は、発信 SIP 端末からの INVITE リクエストと着信 SIP 端末からの 100 Trying レスポンスを攻撃者の SIP 端末が盗聴し、着信側 SIP 端末に偽装した CANCEL リクエストを送信している点は前述の 200 OK レスポンスの偽装と同じである。異なるのは、発信 SIP 端末に 200 OK レスポンスではなく 302 Moved Temporarily レスポンスを送信している点である。この偽装された 302 Moved Temporarily レスポンスによって、発信 SIP 端末は意図しない SIP 端末と通話してしまう可能性がある。

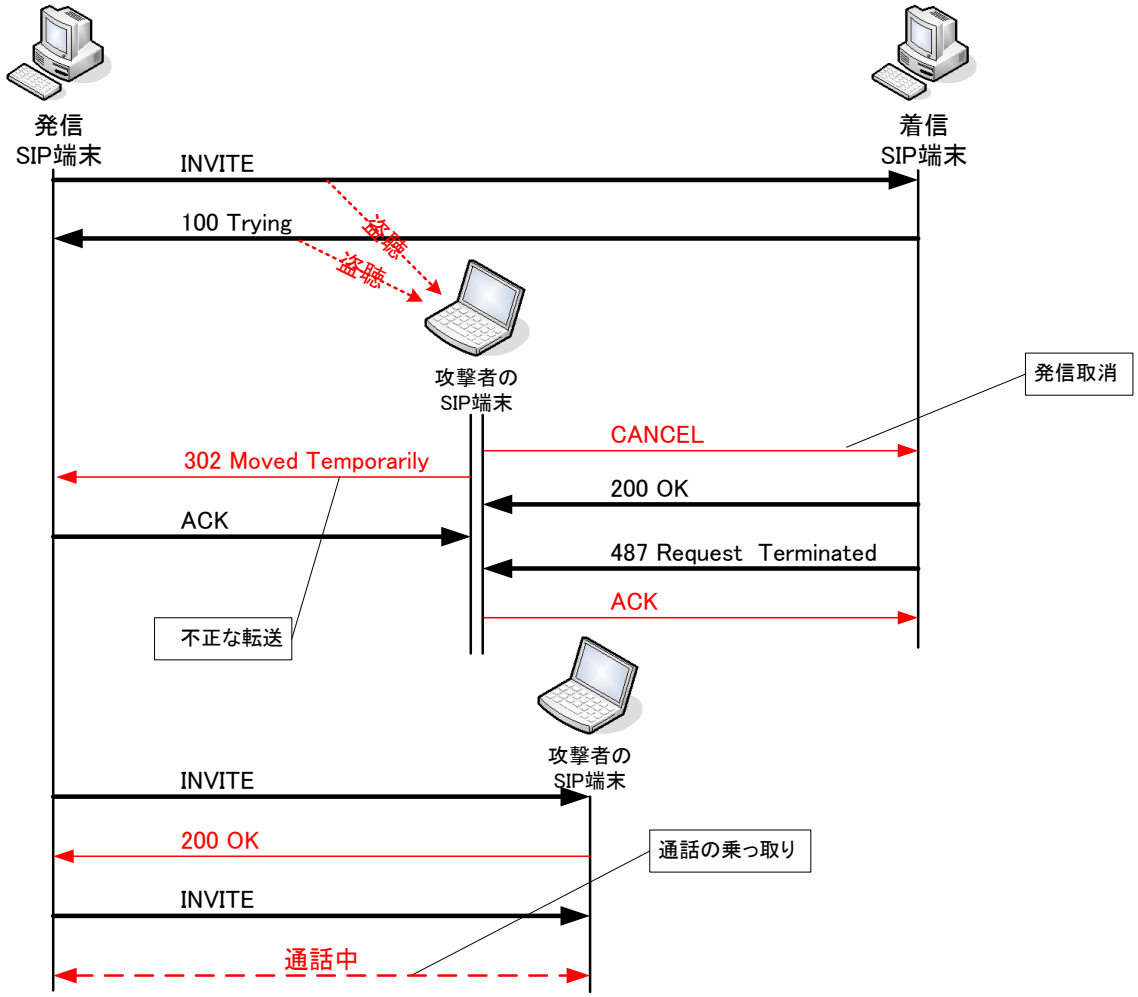


図 2-3 Moved Temporarily レスポンス(一時的移動による着信転送)の偽装

3) 404 Not Found レスポンス(宛先不明)の偽装

本項では、INVITE リクエストに対する 404 Not Found レスポンスの偽装について説明する。

INVITE リクエストに対する 404 Not Found レスポンスは、INVITE リクエストの宛先として記述されている SIP-URI が、SIP サーバに登録されていないことを意味するレスポンスである。例えば、指定した SIP-URI が間違っていたり、受信 SIP 端末が起動していない状態、あるいは、起動はしているがネットワークに接続されていなかったり、ネットワークの障害で通信不能な状態などが考えられる。

404 Not Found レスポンスが偽装された場合、発信者は通信不能と判断して通信をあきらめざるをえなくなる。

【 項目 2. SIP レスポンスの偽装から起こる問題 】

図 2-4 も盗聴と偽装した CANCEL リクエストの送信に関しては、図 2-2/2-3 と同じである。

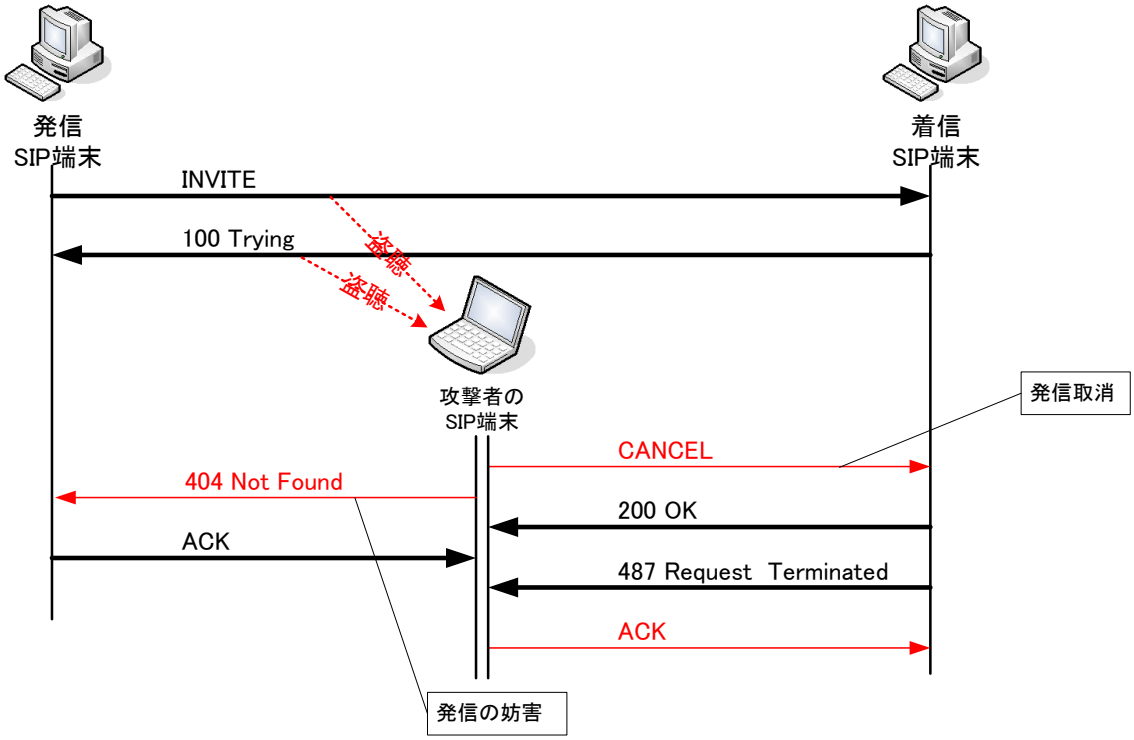


図 2-4 404 Not Found レスポンス(宛先不明)の偽装

【原因と考察】

SIP 認証は、HTTP のダイジェスト認証を利用している。この認証方式は、パスワードをハッシュ値で確認するのでネットワーク上をパスワードが直接送信されることがない。通常 SIP リクエストを SIP サーバや SIP 端末が認証するが、Authentication-Info ヘッダを使って SIP レスポンスを SIP 端末が認証することも可能である。しかし、レスポンスに対する認証は SIP ではほとんど使われていない。これは、SIP を規定する RFC3261 の古いバージョンである RFC2543 で Authentication-Info ヘッダを使わないことになっていたからである。

2.3 対策

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) ファイアウォールや侵入検知システムなど、製品とネットワークとの間にこの脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【 項目 2. SIP レスポンスの偽装から起こる問題 】

【実装ガイド】

1) Secure SIP (SIP over TLS)の実装
2) Authentication-Info ヘッダを使ってレスポンスの認証を行う

2.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol 8.1.3 Processing Responses http://tools.ietf.org/html/rfc3261#section-8.1.1.3

2.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■Ⅰ（注意）	□Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値	2.6		

※前述の 3 つの攻撃手法により受ける深刻度は、いずれも同じ評価結果となった

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□ 隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	■なし	□部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	■なし	□部分的	□全面的

項目3. SIP 認証パスワードの解読

3.1 概要

SIP は HTTP ダイジェスト認証のメカニズムを使用して、リクエストに対して認証を要求することができる。認証情報は SIP のヘッダとしてリクエストに記述されるが、このリクエストをキャプチャされた場合、考えられるパスワードを次々試にしてみて結果を比較するブルートフォースという手法によるパスワード解読が行われる危険がある。パスワードが解読されると、任意の SIP リクエストが作成可能となり、認証要求が無意味となってしまう。

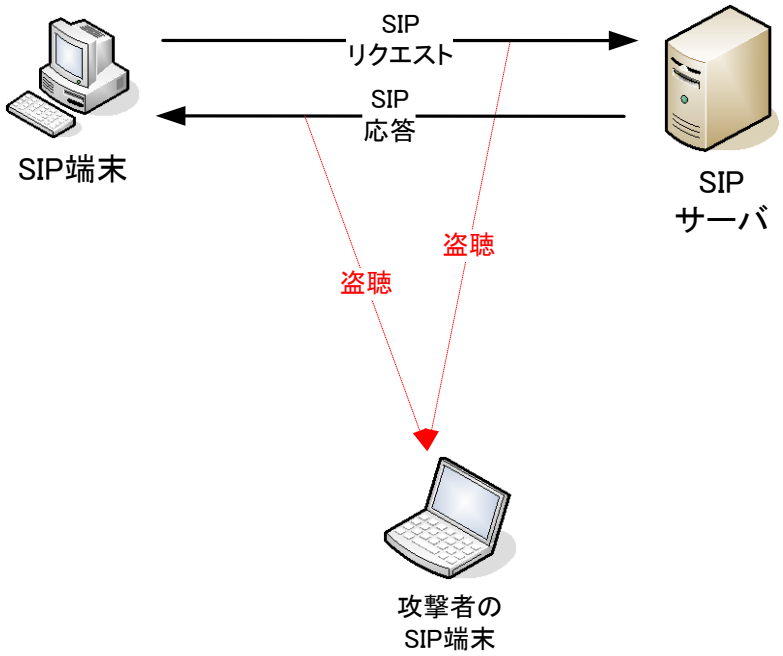


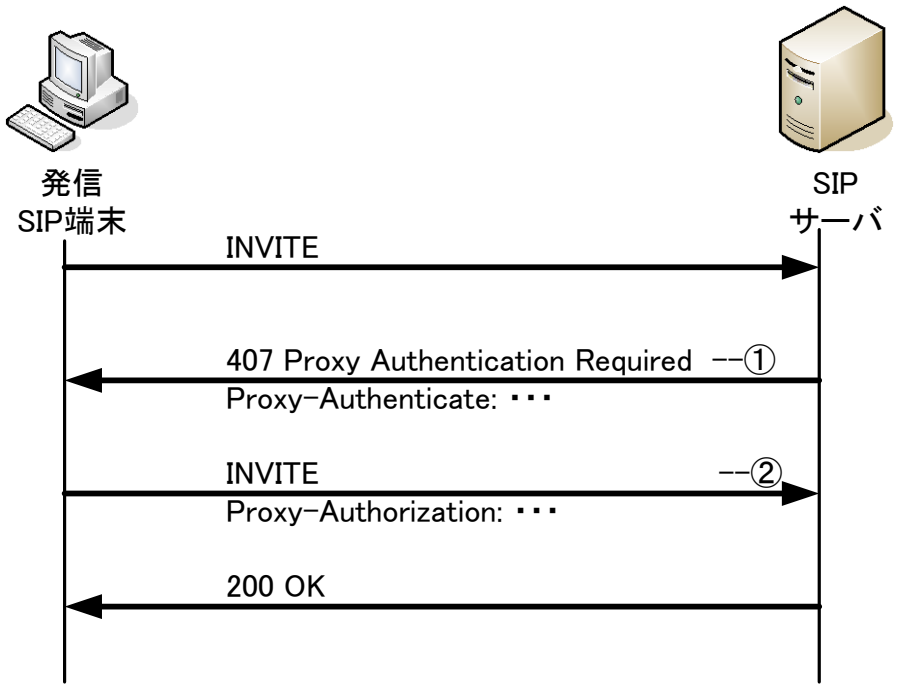
図 3-1 パスワード解析のためのデータ盗聴

3.2 解説

【攻撃手法とその影響】

SIP のリクエストをサーバやクライアント(UAS)が認証する場合、RFC2617 で規定されている HTTP で使用されるダイジェスト認証の仕組みを利用する。ダイジェスト認証はリクエストに対して、認証を求めるサーバやクライアントが 401(Unauthorized)または 407(Proxy Authentication Required)というレスポンスを返すことで始まる。前者のレスポンスには WWW-Authenticate ヘッダが付加され、後者には Proxy-Authenticate ヘッダが付加されている。

【 項目 3. SIP 認証パスワードの解読 】



①

```
407 Proxy Authentication Required
Proxy-Authenticate: Digest realm="atlanta.com",
domain="sip:ss1.carrier.com", qop="auth",
nonce="f84f1cec41e6cbe5aea9c8e88d359",
opaque="", stale=FALSE, algorithm=MD5
```

②

```
INVITE sip: bob@example.com SIP/2.0
Proxy-Authorization: Digest username="Alice", realm="
atlanta.com",
     nonce="c60f3082ee1212b402a21831ae",
     response="245f23415f11432b3434341c022"
```

図 3-2　SIP リクエストの認証

上記のヘッダには”nonce”や”opaque”というパラメータが設定されていて、これらの情報を受け取ったリクエスト送信クライアント(UAC)は、自分のユーザ名とパスワードという秘密情報を加えてハッシュ値といわれる情報を計算する。ハッシュ値を計算する関数は一般にハッシュ関数と呼ばれ、ハッシュ値から、計算の元になった入力値を求めることが非常に困難だという性質を持つ。HTTP や SIP のダイジェスト認証では MD5 というハッシュ関数が使われる。RFC2617 には、MD5 の実装コードサンプルが記述されている。

この関数を使ってハッシュ値を計算する場合、図中のメッセージの他に必要な情報はパスワードだけである。言い換えるとパスワード以外の値は全てメッセージから知ることができる。盗聴者は、順番に予想・生成したパスワードをハッシュ関数に適用し、得られたハッシュ値を、盗聴して得た response パラメータと比較することにより、攻撃者が予想したパスワードが正しいか否かを判断できる。このように総当りで予想したパスワードを比

【 項目 3. SIP 認証パスワードの解読 】

較していけば、時間はかかるがいつかは正しいパスワードを特定できる。このような攻撃手法をブルートフォースと呼ぶ。

SIP パスワードが攻撃者に知られてしまった場合、不正な SIP リクエストが偽装され、登録の改ざん、不正な発信など SIP の機能全般が悪用される可能性がある。

【原因と考察】

ダイジェスト認証は、パスワードそのものを交換せず、nonce などの乱数と、ハッシュ関数の特徴をあわせて利用して、認証処理の安全性を確保しようとする方法である。しかし、SIP のダイジェスト認証では、ハッシュ関数に入力する情報のうちパスワード以外はすべて通信路上で得られるため、パスワードの総当りで解読ができる。また、パスワードの予想には、よくあるパスワード文字列のリストとして、パスワードの候補となる単語や文字列の辞書を利用することで、パスワード解読を高速化する攻撃手法がある。

なお、MD5 という計算方式そのものについては、MD5 自体の脆弱性のため、将来的に利用が推奨されていない。米国政府の情報セキュリティの標準化組織 NIST では、2010 年以降、従来の暗号方式の一部を含めて、ハッシュ関数については MD5 ではなく 256bit の SHA1 または SHA2 という別のハッシュ関数を利用するよう推奨している。これに対して、利用環境やセキュリティの要件に応じて利用基準を設けるべきとする考え方もあり、動向に注意が必要である。

3.3 対策

SIP のダイジェスト認証は、SIP メッセージが暗号化されないまま、容易に盗聴できる環境での利用は避けるべきである。

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) 定期的にパスワードを変更する

【実装ガイド】

1) Secure SIP (SIP over TLS)の実装

【 項目 3. SIP 認証パスワードの解読 】

3.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol 22 Usage of HTTP Authentication http://tools.ietf.org/html/rfc3261#section-22
1999 年 6 月	RFC2617 HTTP Authentication: Basic and Digest Access Authentication http://tools.ietf.org/html/rfc3217
2004 年 8 月	Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD http://eprint.iacr.org/2004/199.pdf
2007 年	IPA - セキュアプログラミング講座 C/C++言語編 第 3 章 計画されたセキュリティ機能 破られにくい暗号技術と擬似乱数の使用 http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c203.html
2008 年 10 月	IPA フォーラム「暗号の世代交代」 http://www.ipa.go.jp/security/event/2008/ipa-forum/documents/IPAforum2008yamagishi.pdf 暗号方式の安全性の評価研究と標準化の動向が詳しい。

3.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■ Ⅰ （注意）	□ Ⅱ （警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値	2.6		

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□ 隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	□なし	■部分的	□全面的
完全性への影響	■なし	□部分的	□全面的
可用性への影響	■なし	□部分的	□全面的

【 項目 4. SIP メッセージボディの改ざんから起こる問題 】

項目4. SIP メッセージボディの改ざんから起こる問題

4.1 概要

SIP メッセージのボディには、その目的により様々なフォーマットが使用される。もっとも一般的なものは SDP と呼ばれる、セッション記述に関するフォーマットである。SDP はセッションのネゴシエーション規則の一部として、メディア(音声や映像)の種類、受信アドレス・ポート、使用されるコーデックなどのパラメータを記述する際に使用される。この他に、INVITE リクエストには、JPEG などの画像データが載ることがある。この JPEG データは着信ユーザに表示される。以下に、これらの情報が改ざんされた場合の脆弱性について記述する。

4.2 解説

【攻撃手法とその影響】

SIP メッセージのボディとして以下の 2 つの場合を考える。

1) INVITE リクエストとそのレスポンスのボディに載る SDP
2) INVITE リクエストのボディに載る JPEG

ボディの改ざんは、ARP テーブルの改ざん等の方法により攻撃者がシグナリングパスに割り込んだり(中間者攻撃)、セッション・ボーダ・コントローラ(SBC)など SIP シグナリングを中継するサーバが乗っ取られる場合などに起こりうる。

1) INVITE リクエストとそのレスポンスに載る SDP

SDP にはメディアの受信アドレス・ポート、メディアの種類、使用されるコーデックなどのパラメータが記述されている

図 4-1 は攻撃者の端末が途中で INVITE リクエストとその 200 レスポンスに記述されている SDP の内容を改ざんすることにより、音声メディアが攻撃者の端末を経由するようになっている状態を表している。この状態では会話の内容は攻撃者に筒抜けになってしまい、図中では、金庫の開錠番号などが不正に取得されている場合を想定している。

【 項目 4. SIP メッセージボディの改ざんから起こる問題 】

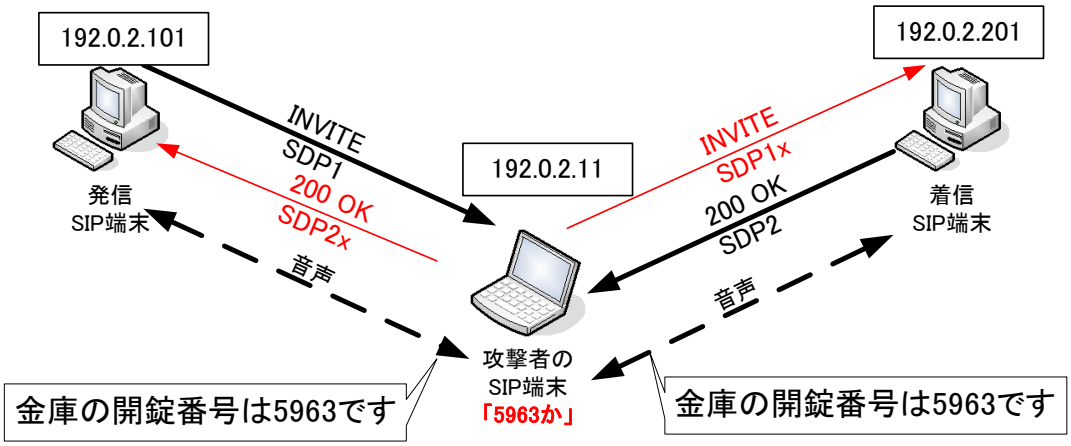


図 4-1 SDP の改ざんによるメディアの第3者中継(通話の盗聴)

1) SDP1

```
v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

2) SDP2

```
v=0
o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com
s=-
c=IN IP4 192.0.2.201
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

3) SDP1x

```
v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.11
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

【 項目 4. SIP メッセージボディの改ざんから起こる問題 】

4) SDP2x

```
v=0
o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com
s=-
c=IN IP4 192.0.2.11
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

図 4-2 SDP の例

図 4-1 は攻撃者の端末がメディアの送信を中継することで、会話の内容が筒抜けになってしまっている例だが、転送時にメディアを変更・改ざん・停止させるなどの介入が可能となる。

2) INVITE リクエストのボディに載る JPEG

INVITE リクエストには JPEG などの画像データが添付されることがある。

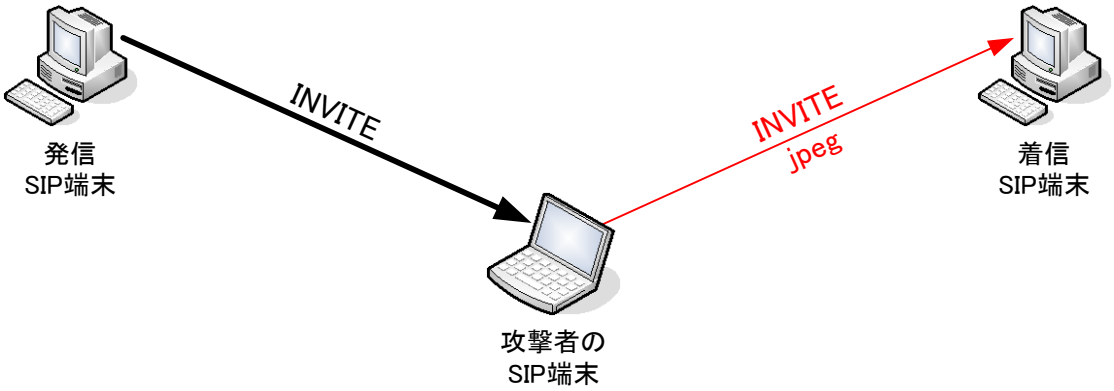


図 4-3 ボディが改ざんされ JPEG が添付される例

図 4-3 は攻撃者の端末によって INVITE リクエストが不正に中継され、ボディに JPEG ファイルが添付されている様子を示している。

図 4-4 はボディに JPEG ファイルが添付された INVITE リクエストの例である。

添付されたファイルはユーザに表示され、発信者の意図しない画像情報が着信ユーザに提示されたり、JPEG ファイルを表示しようとする処理自体がコンピュータにダメージを与える可能性もある。

【 項目 4. SIP メッセージボディの改ざんから起こる問題 】

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
Content-Disposition: render
Content-Type: image/jpeg; name="img10192419528.jpg"
Content-Transfer-Encoding: base64
Content-Length : 951

/9j/4AAQSkZJRgABAgEASABIAAD/2wBDAAYEBAQFBAYFBQYJBgUGCQsIBgYICwwKCgsKCgwQ
DAwMDAwMEAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAz/2wBDAQcHBw0MDRgQEBgUDg4O
...
```

図 4-4 ボディが JPEG の例

【原因と考察】

SIP メッセージのボディが不正に改ざんされる原因は、以下の 3 つが考えられる。

1) パケットが盗聴される
2) SIP メッセージが不正に中継される
3) SIP メッセージの改ざんを検証していない

4.3 対策

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) IP レベルの改竄に対する対策

SIP メッセージが不正に中継されることを防ぐためには、IP ネットワークのルーティングテーブルの改ざんや、ARP テーブルの不正操作、DNS ポイズニング（不正書き換え)などへの対策が必要となる。

【実装ガイド】

1) Secure SIP (SIP over TLS)の実装
2) S/MIME により End-to-End の暗号化を行う

【 項目 4. SIP メッセージボディの改ざんから起こる問題 】

4.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol http://tools.ietf.org/html/rfc3261
2006 年 7 月	RFC4566 SDP: Session Description Protocol http://tools.ietf.org/html/rfc4566

4.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■ Ⅰ（注意）	□ Ⅱ（警告）	□ Ⅲ（危険）
本脆弱性の CVSS 基本値	2.6		

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□ 隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	■なし	□部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	■なし	□部分的	□全面的

【 項目 5. 保護されていないトランスポートプロトコルを選択させられる問題 】

項目5. 保護されていないトランスポートプロトコルを選択させられる問題

5.1 概要

SIP で TLS 接続を開始する際の TCP 接続時に、TCP 接続失敗を示すレスポンスパケットを受信すると、SIP メッセージの送信を TLS ではなく、保護されていない UDP による送信に切り替えてしまうことがある。

5.2 解説

SIP はメッセージを送信するトランスポートプロトコルとして、TCP,UDP の他にセキュリティを考慮したプロトコルである TLS を使用することも仕様として決められている。

【攻撃手法とその影響】

TLS での接続を開始する場合、まず TCP による接続を行う。この TCP 接続確立手順に攻撃者が介入することで、TCP 接続の確立を失敗させ、TCP 接続の失敗に関する RFC の追加手順を悪用することで、UDP プロトコルの使用に誘導し盗聴やなりすましが容易になってしまう。

図 5-1 では、まず発信 SIP 端末が、INVITE リクエストを送信するトランスポートとして使用する TLS の接続手順のために SYN フラグの立った TCP の接続要求パケットを送信している。

攻撃者の SIP サーバあるいは SIP 端末はこの TCP の接続要求パケットに対して TCP の RST フラグが立ったパケットか ICMP(Protocol Unreachable)を送信する。

発信側 SIP 端末は、この TCP パケットあるいは ICMP を受信したことにより、TCP 接続が失敗したと判断し、RFC3261 に対する記述の誤解から UDP で SIP リクエストを再送信しようとする。

【 項目 5. 保護されていないトランスポートプロトコルを選択させられる問題 】

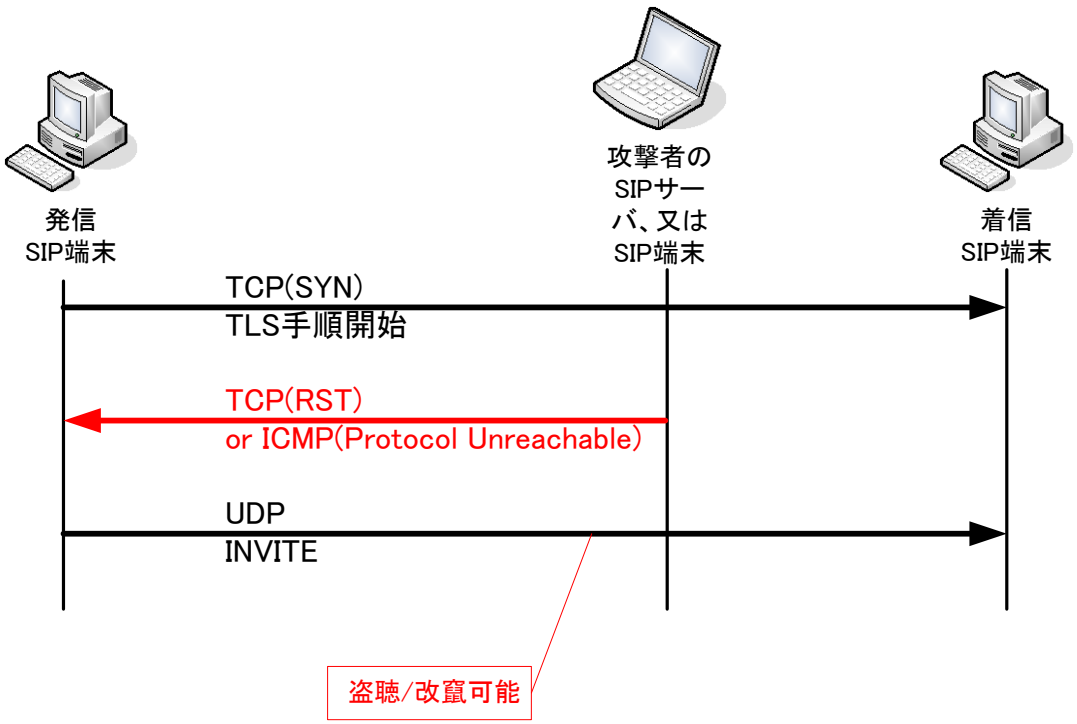


図 5-1 UDP へのダウングレード

【原因と考察】

RFC3261 の「18.1.1 リクエストの送信」にはトランスポートのダウングレードに関して以下のような記述がある。

「端末が大きなサイズのメッセージを送る場合、UDP 送信に関するメッセージサイズの制限のために、そうでなければ UDP で送られた筈のリクエストを TCP 上で送った場合、コネクションを確立する試みが ICMP Protocol Not Supported を生成するか TCP のリセットを招く結果になるなら、エレメントは UDP を使ってリクエストを再試行するべきである [SHOULD]。これは、TCP をサポートしない RFC2543 準拠の実装との下位互換を提供するためだけである。この仕様の今後の改定において、この動作は反対されることが予想される。」

RFC3261 の旧バージョンである RFC2543 では TCP のサポートがオプションであったため下位互換性への配慮から RFC3261 には上記のようなトランスポートのダウングレード規定が含まれる。

TLS も TCP の接続で開始されることから、発信側 SIP 端末が無条件にこの記述に従って動作した場合、悪意のある SIP サーバ/端末が TCP(RST)か ICMP(Protocol Unreachable)を送信することで、TCP の接続を UDP にダウングレードさせられる可能性がある。

RFC3261 の「18.1.1 Sending Requests」に記述されているトランスポートのダウングレードに関する記述は、あくまでも TCP での接続に関する下位互換性を考慮した内容であり、TLS の接続手順の一部である TCP 接続の失敗が UDP での接続を強制するものではない。記述の前提も UDP での送信に関して安全上の懸念がない場合なので、発信側 SIP 端末は TLS を UDP にダウングレードすべきでない。

また、ネットワーク自体が安全でない環境では TCP-RST 自体の偽装は防ぐのは難しいことも問題である。

【 項目 5. 保護されていないトランスポートプロトコルを選択させられる問題 】

5.3 対策

【運用ガイド】

1) 運用条件を明確にして、利用するトランスポート方式をサーバで制限する
2) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
3) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
4) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【実装ガイド】

1) RFC の仕様に沿った実装をする
使用される状況に適合した運用条件を守ることに留意し、TCP（RST）や ICMP(Protocol Unreachable 等)の受信で無条件に UDP へのダウングレードを行わない

5.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol 18.1.1 Sending Requests http://tools.ietf.org/html/rfc3261#section-18.1.1
2007 年 3 月	Sipera への報告 SIP compliant clients may be vulnerable to transport rollback vulnerability http://www.sipera.com/index.php?action=resources,threat_advisory&tid=178&

5.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■ Ⅰ （注意）	□ Ⅱ （警告）	□Ⅲ （危険）
本脆弱性の CVSS 基本値	2.6		

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□ 隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	□なし	■部分的	□全面的
完全性への影響	■なし	□部分的	□全面的
可用性への影響	■なし	□部分的	□全面的

【 項目 6. DoS 攻撃による SIP のサービス妨害 】

項目6. DoS 攻撃による SIP のサービス妨害

6.1 概要

DoS(Denial of Service)や DDoS(Distributed Denial of Service)と呼ばれる攻撃手法は、SIP にも適用できる。意味のないリクエストを大量に作成し送りつける、あるいは別の SIP サーバを使って攻撃メッセージを増幅させるなどの手法により、攻撃対象ホストの処理能力を低下させることできる。

※ 関連する脆弱性として「項目 12. 不具合を起こしやすいパケットに対応できない問題」がある。DoS には、SIP として意味のないリクエストと、SIP としての体裁は整っているが、本来送られないはずのリクエストを使う場合がある。本節では後者に関する脆弱性を対象とする。

6.2 解説

【攻撃手法とその影響】

単純な DoS の手法は、偽装されたリクエストやレスポンスを攻撃対象の SIP 端末に直接送信することである。これはサーバ認証への対応などが必要なく比較的難易度は低いと考えられる。一方閉じたネットワーク内に存在する SIP 端末を攻撃対象とする場合は、出入り口として存在する SIP サーバを経由した攻撃となる。或いは SIP サーバ自体を攻撃対象とした場合の方がシステム全体に与えるインパクトは大きいと考えることもできる。ここでは、いろいろ考えられる攻撃手法の中で RFC3261 の「26.1.5 サービス拒否および増幅」に記述されている二つの DoS 攻撃手法を例として考える。

1) SIP サーバを介した SIP レスポンスによる攻撃

図 6-1 は、攻撃者の SIP 端末が INVITE リクエストを偽装する際に、攻撃対象となる SIP 端末の IP アドレス(1.1.1.1)とポートを SIP リクエストの Via ヘッダに設定し、攻撃の仲介役として利用する SIP サーバまたは端末に送信することで、身に覚えのないレスポンスが攻撃対象の SIP 端末に集中している状態を示している。レスポンスは、攻撃に利用される端末あるいはサーバの設定によって、180, 200, 401 または 407 などが考えられるが、攻撃目標となる SIP 端末に不正なレスポンスが送信される点で違いはないと考えられる。

【 項目 6. DoS 攻撃による SIP のサービス妨害 】

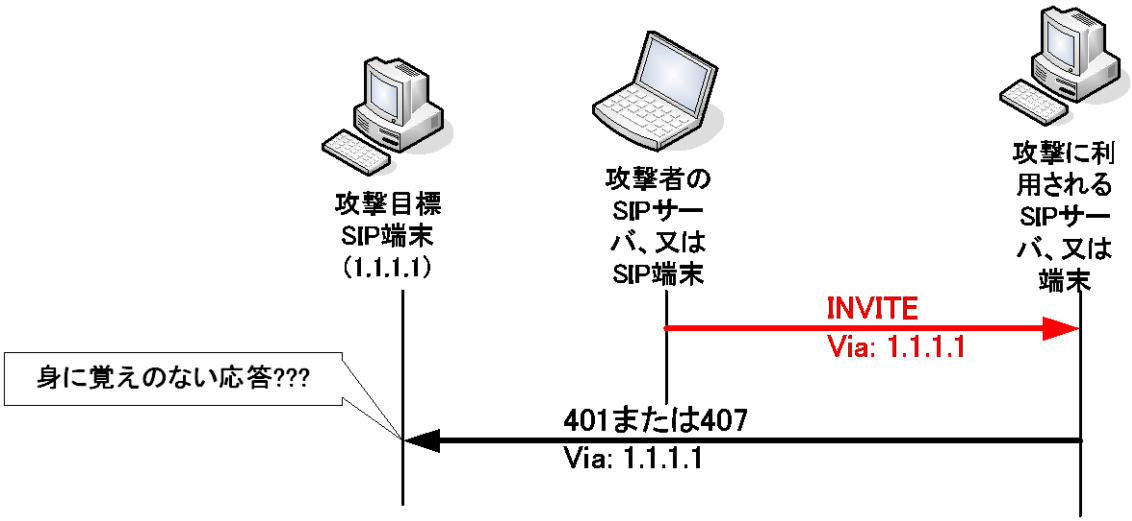


図 6-1 レスポンスによる攻撃

2) SIP サーバを介した SIP リクエストによる攻撃

図 6-2 は、攻撃者の SIP 端末が INVITE リクエストを偽装するさいに、攻撃対象となる SIP 端末の IP アドレス(1.1.1.1)とポートを SIP リクエストの Route ヘッダに設定し、攻撃の仲介役として利用される SIP サーバに送信することで、無意味な SIP リクエストが攻撃対象の SIP 端末に集中している状況を表している。攻撃目標への送信は Route ヘッダによって決定されるので、リクエスト内の宛先を表す SIP-URI は、必ずしも攻撃目標を特定するものである必要は無い。しかし、図中に示すように、攻撃に利用される SIP サーバによってフォークされるような SIP-URI を選択することで、リクエストを増幅し攻撃効果を大きくすることも可能である。

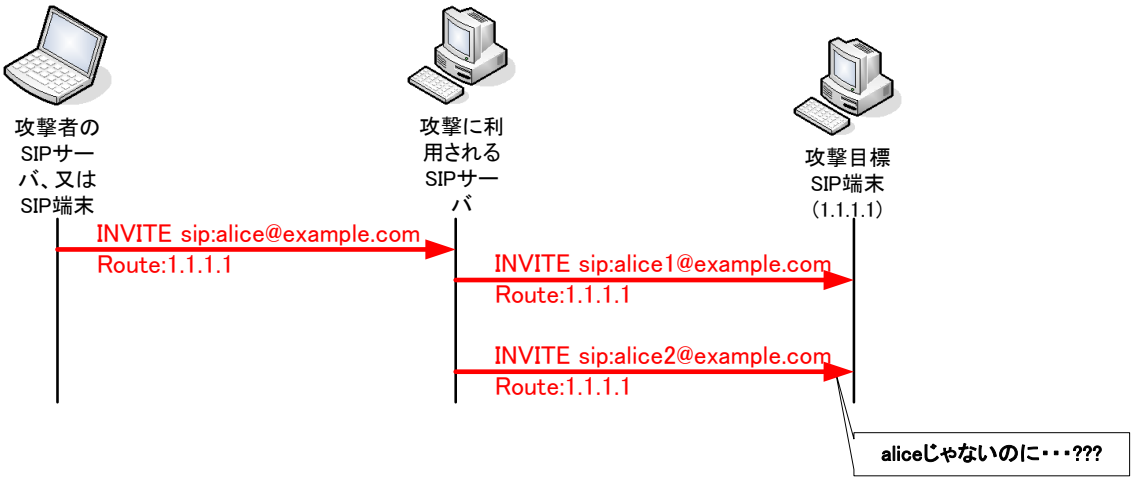


図 6-2 リクエストによる攻撃

これらの攻撃を受けることにより、SIP 端末はリクエストやレスポンスに対する処理能力が低下し、サービス不能の状態になる可能性がある。

【 項目 6. DoS 攻撃による SIP のサービス妨害 】

【原因と考察】

攻撃に使われる SIP リクエストや SIP のレスポンスについて、SIP の規定に従った破棄処理を行うことは準正常系の処理として、ほとんどの場合実装されているはずである。この種の攻撃の目的は偽装したリクエストやレスポンスによって標的となる SIP 端末やサーバを操作することではなく、過度の処理負荷によって処理能力を低下させることにある。この点から、攻撃パケットが SIP 的な処理に渡されないような対策が有効と考えられる。

6.3 対策

【運用ガイド】

1) 特定のアドレス・ポートにパケットが集中した際には、パケットの転送を制限するようなルータを配置する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【実装ガイド】

1) 処理の制限
受信した IP パケットを、SIP のリクエストやレスポンスとして処理する前に、1 秒間のリクエスト処理数など、実装要件から決定された上限値を超える場合は、SIP のリクエストやレスポンスを処理せずに廃棄する。また、上限値を超えるリクエストのソース IP アドレスを記録し、運用者が確認できる機能を提供することが望ましい。

6.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol 26.1.5 Denial of Service and Amplification http://tools.ietf.org/html/rfc3261#section-26.1.5
2008 年 9 月	IP 電話に無言電話が着信する現象が多発, 原因はインターネット上からの不正攻撃 http://itpro.nikkeibp.co.jp/article/NEWS/20080910/314570/ 「NTT コミュニケーションズでは不正アクセスを遮断する措置をとった」、と報じられている。
2008 年 9 月	「ヤマハの音とネットワーク製品を語る」ブログ トラブル対策-不正な SIP 着信?(3) http://projectphone.typepad.jp/blog/2008/09/-sip3-fcee.html 2008 年 9 月に発生した「SIP 不正アクセスの通信内容」のシーケンスチャート
2008 年 9 月	FAQ for YAMAHA RT シリーズ 無言電話/ 不正な SIP パケットに対策するための設定例 http://www.rtpro.yamaha.co.jp/RT/FAQ/VoIP/troublevoip-ans.html#9 特定のユーザか発番号からの呼だけに着信する設定が紹介されている。 FUSION IP-Phone への無言電話多発の対応策について http://www.fusioncom.co.jp/oshirase/20080909_2.html

【 項目 6. DoS 攻撃による SIP のサービス妨害 】

2008 年 11 月	VoIP/SIP エンティティに対する DoS アタック http://itpro.nikkeibp.co.jp/article/COLUMN/20081028/317888/ 日本製 SIP 脆弱性検査ツールを開発・販売する NextGen ネットワークセキュリティ事業本部長による日本語の解説
2008 年 12 月	RFC5393 Addressing an Amplification Vulnerability in SIP Forking Proxies http://tools.ietf.org/html/rfc5393 SIP Proxy がリクエストを 2 つ以上に分岐させるときは、ループ検出を行うよう注意を求める資料。

6.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■ Ⅰ（注意）	□ Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値	2.6		

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□ 隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	■なし	□部分的	□全面的
完全性への影響	■なし	□部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

【 項目 7. その他 SIP 拡張リクエストの脆弱性 】

項目7. その他 SIP 拡張リクエストの脆弱性

7.1 概要

SIP のリクエストは、RFC3261/3262 以外の RFC で拡張のリクエストが定義されている。

SIP メソッド	内容
INFO	セッション内の情報通知
SUBSCRIBE	状態情報の要求
NOTIFY	状態情報の通知
UPDATE	セッションの変更
REFER	リクエストの送信指示
MESSAGE	テキストメッセージ等の送信
PUBLISH	状態情報の通知

これらのメッセージが偽装された場合の影響について説明する。

7.2 解説

【攻撃手法とその影響】

攻撃手法として盗聴あるいは SIP 以外の手段で取得した SIP-URI に偽装したリクエストを送信することがあげられる。

図 7-1 は、偽装された MESSAGE リクエストにより、偽の業務連絡が送られる例である。

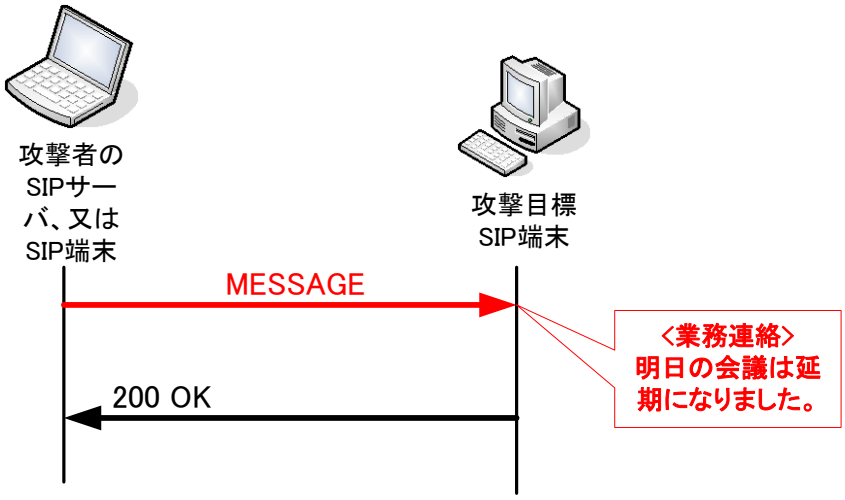


図 7-1 偽装されたメッセージによる偽の業務連絡

その他の SIP リクエストについても、その役割と偽装されたさいの影響を表 7-1 にまとめる。

【 項目 7. その他 SIP 拡張リクエストの脆弱性 】

表 7-1　SIP リクエストの役割と偽装の影響

リクエスト	役割と影響	
INFO	役割	INFO リクエストはトーン信号(DTMF)の送信に使用されることが考えられるが、その他の使い方は特に決められてはいない。
	影響	トーン信号を偽造された場合、IVR(音声自動応答装置)などに対する意図しない入力信号が送信され、情報の改変や漏洩が起こる可能性がある。 また、着信音の鳴り分けなどに利用された場合は着信先が偽られる可能性がある。
SUBSCRIBE	役割	指定した情報の通知を NOTIFY リクエストで通知されるように依頼するためのリクエスト。
	影響	SUBSCRIBE リクエストが偽装された場合、閲覧が許可されていない攻撃者にプレゼンス情報が送信される可能性がある。あるいは、閲覧が許可されている端末に対するプレゼンス情報の配信が中止させられる可能性がある。
NOTIFY	役割	SUBSCRIBE リクエストにより依頼された情報を、通知するためのリクエスト。多くの場合、通知する情報はボディに記述される。
	影響	NOTIFY リクエストが偽装された場合、配信されたプレゼンス情報などが改ざんされている可能性があり、オンライン状態なのにオフライン状態であるかのような間違った情報に基づいてユーザの判断がなされてしまう可能性がある。
UPDATE	役割	セッションの変更や更新のために使用されるリクエスト。
	影響	UPDATE リクエストが偽装された場合、メディアの送信停止や、攻撃者の端末との通信に誘導される可能性がある。
REFER	役割	新しいリクエストを生成するように指示するリクエスト。多くの場合、転送のための INVITE リクエストの生成を指示するために使用される。 最近では、PoC(Push to talk over Cellular：一人が発言権を持つ形式の会議サービス)のシグナリングに利用される場合もある。
	影響	REFER リクエストが偽装された場合、通話が意図しない相手に転送されてしまう可能性がある。
MESSAGE	役割	ボディに任意の情報を載せて送信されるリクエスト。テキストチャットなどに利用される。
	影響	MESSAGE リクエストが偽装された場合、なりすました相手とのチャットが行われ、攻撃者に不適切な情報を送信してしまったり、攻撃者から偽装された情報を受信してしまう可能性がある。
PUBLISH	役割	NOTIFY リクエストと同じく、情報を通知するためのリクエストでだが、SUBSRIBE リクエストによる動的通知依頼を必要とせず、アプリケーションの設定に従って情報の種類と送信先が決められる。
	影響	PUBLISH リクエストが偽装された場合、通知されたプレゼンス情報などが改ざんされている可能性があり、オンライン状態なのにオフライン状態であるかのような間違ったプレセンス情報に基づいてユーザの判断がなされてしまう可能性がある。

【原因と考察】

盗聴や、SIP 以外の手段により認証のパスワードが漏洩したり、リクエストの送信に必要なリクエスト URI やダイアログ ID などが取得されることが原因と考えられる。

【 項目 7. その他 SIP 拡張リクエストの脆弱性 】

7.3 対策

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【実装ガイド】

1) Secure SIP (SIP over TLS)の実装

7.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol http://tools.ietf.org/html/rfc3261
2002 年 6 月	RFC3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP) http://tools.ietf.org/html/rfc3262
2002 年 6 月	RFC3265 Session Initiation Protocol (SIP)-Specific Event Notification http://tools.ietf.org/html/rfc3265
2000 年 10 月	RFC2976 The SIP INFO Method http://tools.ietf.org/html/rfc2976
2002 年 9 月	RFC3311 The Session Initiation Protocol (SIP) UPDATE Method http://tools.ietf.org/html/rfc3311
2002 年 12 月	RFC3428 Session Initiation Protocol (SIP) Extension for Instant Messaging http://tools.ietf.org/html/rfc3428
2003 年 4 月	RFC3515 The Session Initiation Protocol (SIP) Refer Method http://tools.ietf.org/html/rfc3515
2004 年 10 月	RFC3903 Session Initiation Protocol (SIP) Extension for Event State Publication http://tools.ietf.org/html/rfc3903
2007 年 9 月	OMA Push to talk Over Cellular V1.0.2 Approved Enabler http://www.openmobilealliance.org/release_program/poc_v1_0.html

【 項目 7. その他 SIP 拡張リクエストの脆弱性 】

7.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■Ⅰ（注意）	□Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値	2.6		

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	■なし	□部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	■なし	□部分的	□全面的

【 項目 8. RTP メディアの盗聴から起こる問題 】

項目8. RTP メディアの盗聴から起こる問題

8.1 概要

RTP のメディアストリームは盗聴、傍受されることがある。オープンソースのパケットキャプチャソフトを利用すると、簡単な操作で IP 電話用の音声ストリームを取り出して再生できる。

8.2 解説

【攻撃手法とその影響】

他のホストのパケットを取り出せる環境で、RTP メディアストリームを含む IP パケットのキャプチャを行う。キャプチャしたパケットから、RTP メディアストリームを特定し、その中から音声やビデオ、テキストなどのメディアデータを取り出すことができる。

オープンソースで無料のパケット解析ソフトウェアを利用するだけでも、IP 電話の通話前後のパケットをキャプチャしたあと、双方の話者の音声を簡単に再生できる。

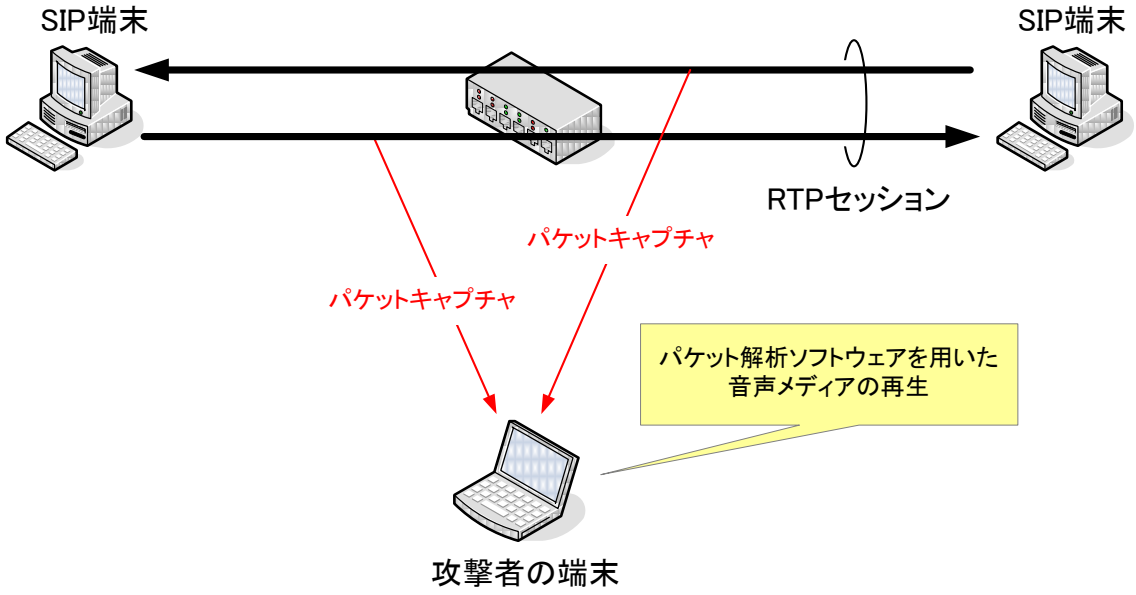


図 8-1 RTP メディアの盗聴

パケット解析ソフトとは、ネットワークの詳細な動作確認、トラブル対策ツールとして、よく利用されており、ネットワーク関連業務のための必携ツールともいえる。パケット解析ソフトは有料の市販品も存在するが、オープンソースのパケット解析ソフトウェアでも、メニューやボタンを選択するだけで簡単に RTP の音声メディアストリームをキャプチャして再生することができる。

ここで盗聴の対象となる RTP メディアストリーム上で、転送されるメディアの例には次のようなものがある。

【 項目 8. RTP メディアの盗聴から起こる問題 】

1) IP 電話: 音声、またはプッシュ番号(ダイアルトーン信号、DTMF 信号)
2) テレビ電話、テレビ会議: 音声とビデオ
3) マルチメディア会議: 音声、ビデオ、アプリケーションの画面、操作イベント等

RTP メディアストリームの盗聴によって、上記のような情報が第三者に暴露されることになる。具体的な盗聴内容としては、IP 電話の通話中の会話、IP 電話で音声自動応答システム(IVR)などに入力するプッシュ番号、テレビ会議でのビデオカメラの映像やアプリケーションの画面例、などである。

RTP メディアはこのほかにもさまざまなメディアに拡張されている。拡張された RTP メディアの種類については IETF Audio/Video Transport (avt)ワーキンググループ※を参照してほしい。

※ IETF Audio/Video Transport (avt)ワーキンググループ
http://ietf.org/html.charters/avt-charter.html

また、RTP パケットには、RTP を制御するための、RTCP(リアルタイム制御プロトコル: Realtime Control Protocol)の情報も含まれているため、RTP メディアと同様に、RTP の品質レポートや RTP の発信者情報なども露出する。RTCP の詳しい内容については「[参照]10. RTCP の偽装から起こる問題」を参照されたい。

【原因と考察】

RTP が暗号化されていないため、盗聴の危険があることは、RTP の RFC1889(1996 年 1 月)の"9. Security"、"9.1 Confidentiality"で指摘されている。RTP の標準では、RTP 内での DES 暗号方式の利用が示唆されているが、実際は IPsec などの RTP より低いレイヤでの保護機能の利用が期待されていた。

RFC1889 の改版である RFC3550 では、RTP メディアストリームの保護のために SRTP(Secure RTP、その後 RFC3711 として標準化)の利用が推奨されている。

しかし、RTP と SRTP はともに暗号化については定義しているものの、暗号化やメッセージ署名のための鍵の生成や、安全な鍵の交換については定義していなかった。その後、2004 年には MIKEY という鍵交換プロトコルが RFC3830 として標準化されたが、鍵交換に証明書が必要になるなど、実用的でないことから、SRTP 用の鍵交換方法としては普及していない。一方、現実の世界では SDP 上に鍵をそのまま記述して転送する方法が、一般の IP 電話機器で普及するようになった。このように、現在に至るまで、RTP メディアストリームを保護するための課題は鍵の交換方法に残されている。

RTP メディアストリームの保護についてはいくつかの方法が並存して提唱されている。特に RTP に関連する主な対策方法を紹介することで、今後の見通しの参考にしていただきたい。

1) SRTP (鍵交換は MIKEY など別標準に依存)： RTP ペイロードの保護
2) ZRTP： RTP ペイロードの保護と鍵交換
3) RTP over DTLS と SRTP での DTLS 鍵の利用： UDP ペイロードの保護と鍵交換
4) **メディアコンテンツ自体の保護**： サウンド、ビデオデータそのものの暗号化など

1) SRTP

SRTP[RFC3711]は音声やビデオのようなリアルタイムな転送処理のために、RTP パケットのうち、保護する対象をできるかぎり最小限にとどめた方式である。IPsec では最大で、IP パケット全体が暗号化されるが、SRTP では RTP ペイロードのみが暗号化される。

【 項目 8. RTP メディアの盗聴から起こる問題 】

もともと RTP には DES 暗号方式を利用した暗号化方式が定義されていたが、DES は暗号強度が不足し、時代遅れになっていた。SRTP では、組込機器にも実装しやすく高速処理が可能な AES(Advanced Encryption Standard)暗号方式が標準となっている。また、無線 LAN のようにパケットの欠落(パケットロス)が起こりやすい環境でも利用しやすいよう、AES のカウンタモードが採用されている。

ただし、SRTP では、暗号やメッセージ署名に使う、暗号鍵の交換方法を定めていない、という問題がある。2007 年 8 月現在の SRTP を実装した機器において、SRTP 用の鍵を配布する方法は、主に SIP の SDP 上に crypt 属性の値として記述されていることが多い。このような方法を業界では”sDescription(SDES)での鍵配布”などと呼んでいる。このように SDP 上に生のテキスト形式で鍵を記述して配布するとき、SDP を転送する SIP プロトコルが TLS や IPsec で保護されていないと、SIP の SDP に書かれた鍵の値はネットワーク上に露出することになり、SRTP の鍵が第三者の手に渡ることになる。

SRTP で使う鍵を安全に交換する方法として MIKEY が標準化されているが、MIKEY は鍵を自動的に生成する機能が SIP と連動していないことや、RTP の利用開始時に証明書の処理を行ったり、鍵を交換するために時間がかかってしまうなどの問題がある。

2) ZRTP

ZRTP(Media Path Key Agreement for Secure RTP)は電子メールの暗号化方式である PGP を開発した Phil Zimmerman(フィル・ジンマーマン)が提案する RTP の保護方式である。

ZRTP の特徴は、RTP を暗号化するための鍵を、RTP のメディアストリームを転送する初期段階に、RTP メディアストリームから決定・交換するというユニークなものである。そのため、RTP の初期段階では、RTP メディアが保護されないが、鍵交換が完了したあとは暗号化やメッセージ署名を使って RTP メディアストリームを保護できるようになる。また、SIP とは関係なく RTP 上だけで鍵生成と交換を行うため、既存の RTP 対応製品のメディアストリームの間に挿入する形で利用することもできる(Zfone)。

3) RTP over DTLS と、SRTP での DTLS 鍵の利用

まず、DTLS (Datagraram TLS) は、もともと TCP 上だけで利用できた TLS(Transport Layer Security)を拡張し、UDP を保護できるようにした方式である。

RTP over DTLS は、UDP ペイロードにあたる RTP のヘッダとボディを DTLS を使って保護する提案だが、RTP over DTLS は SRTP と比べると鍵生成と鍵交換の処理が重く、音声やビデオなどのリアルタイムなメディア転送には向いていない。一方、SRTP は暗号を利用してメディアを安全に転送する機能を提供するが、暗号で利用するための鍵を安全に交換する方法は定義しておらず、SRTP を利用する場合は、MIKEY などの独自の鍵交換処理が必要になる。そこで、UDP 上の DTLS で安全に生成・交換された鍵を SRTP で利用する提案※がある。

※ Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)
http://tools.ietf.org/html/rfc5763

SRTP の鍵交換方式には MIKEY や ZRTP、DTLS-SRTP などが提案されているが、2007 年 3 月の IETF 会合での非公式集会「RTP Secure Keying BoF(Birds Of a Feather)」で、DTLS-SRTP を中心に検討する方向が打ち出されている。

DTLS を利用するメリットとして、ベースとなっている TLS が広く普及しており相互運用性が高いことと、SSL 開発以来の長年の運用を経て、公開鍵暗号を利用した SSL/TLS の事故の少なさが認められている背景がある。また、開発者向けのメリットとしては、TLS

【 項目 8. RTP メディアの盗聴から起こる問題 】

を利用したアプリケーションは、暗号通信の初期化中や通信中に、いつでも暗号通信に関するエラーや攻撃の検出情報が受け取れる点がある。このようにアプリケーションが独自に暗号通信の制御を行える特長は IPsec にはないメリットであり、特にさまざまな機器と通信しなければならない SIP 環境では重要である。

なお、DTLS-SRTP では、SIP のシグナリングについては別途 TLS などを利用する形となっており、SIP と RTP の保護が別々にできるようになっている。この理由は、SIP が何段ものホップバイホップの通信を保護するのに対して、RTP は直接対向する端末同士のエンドツーエンドの通信を保護するためである。

4) メディアコンテンツ自体の保護

メディアストリーム上で転送される、音声データやビデオデータ自体に、視聴者だけが知っている鍵などで暗号化を行い、保護する方法も考えられる。一般に DRM(Digital Rights Management: デジタル著作権保護)と呼ばれる技術やシステムが該当する。DRM などのメディアコンテンツ自体を保護する方法は、RTP 以外の方法での保護となるため、RTP そのものには、SRTP などの保護機能は不要になることもある。

8.3 対策

【運用ガイド】

1) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
2) IPsec、SSL-VPN などの暗号化トンネルを使って SIP/RTP 通信を保護する

【実装ガイド】

1) Secure RTP (SRTP)の実装
   保護対象が RTP ペイロードだけで十分ならば、SRTP を利用するのが適当である。
2) RTP を利用した製品自体が保護機能を持たない、あるいは SRTP を利用したときに鍵配送が保護されていないなど、通信の保護機能がネットワークや下位レイヤの機能に依存する場合は、製品利用者への注意喚起が必要である。

SRTP を利用できる場合は他の RTP 製品との互換性に配慮が必要である。特に、SRTP については脆弱な暗号化方法を選択させられる、などの危険性も指摘されており、新たな脆弱性を組み込まないよう注意が必要である。

【 項目 8. RTP メディアの盗聴から起こる問題 】

8.4 参考情報

公開年月	情報源
1996 年 1 月	RFC1889 RTP: A Transport Protocol for Real-Time Applications(旧版) 9. Security http://tools.ietf.org/html/rfc1889#section-9
2003 年 7 月	RFC3550 RTP: A Transport Protocol for Real-Time Applications(最新版) 9. Security http://tools.ietf.org/html/rfc3550#section-9
2003 年 7 月	RFC3551 RTP Profile for Audio and Video Conferences with Minimal Control http://tools.ietf.org/html/rfc3551
2004 年 3 月	RFC3711 The Secure Real-time Transport Protocol (SRTP) http://tools.ietf.org/html/rfc3711
2004 年 8 月	RFC3830 MIKEY: Multimedia Internet KEYing http://tools.ietf.org/html/rfc3830
2006 年 4 月	RFC4347 Datagram Transport Layer Security (DTLS) http://tools.ietf.org/html/rfc4347
2007 年 6 月	3GPP TS　33.203 3G security; Access security for IP-based services http://www.3gpp.org/ftp/Specs/html-info/33203.htm
2007 年 7 月	IETF Audio/Video Transport (avt)ワーキンググループ http://ietf.org/html.charters/avt-charter.html RTP プロトコルと RTP ペイロードで転送するメディアを定義。
2007 年 7 月	ZRTP: Media Path Key Agreement for Secure RTP http://tools.ietf.org/html/draft-zimmermann-avt-zrtp
2007 年 4 月	Asterisk encryption http://www.voip-info.org/wiki/view/Asterisk+encryption Asterisk で SRTP を利用するための設定、互換機器・ソフトなど。
2007 年 10 月	The Zfone Project http://zfoneproject.com/ PGP の作者、Phil Zimmermann 氏の ZRTP を利用した Zfone を配布。
2007 年 10 月	Sipera への報告 Vonage voice conversation may be vulnerable to eavesdropping http://www.sipera.com/index.php?action=resources,threat_advisory&tid=359 米国 Vonage の IP 電話サービスで、音声パケットが暗号化されていない問題。
2010 年 5 月	RFC5763 - Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS) 6.10.　Media over SRTP http://tools.ietf.org/html/rfc5763#section-6.10
2010 年 5 月	RFC5764 - Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP) http://tools.ietf.org/html/rfc5764

【 項目 8. RTP メディアの盗聴から起こる問題 】

8.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■Ⅰ（注意）	□Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値	2.6		

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響 （情報漏えいの可能性）	□なし	■部分的	□全面的
完全性への影響 （情報改ざんの可能性）	■なし	□部分的	□全面的
可用性への影響 （業務停止の可能性）	■なし	□部分的	□全面的

【 項目 9. RTP メディアの偽装から起こる問題 】

項目9.　RTP メディアの偽装から起こる問題

9.1　概要

すでに確立された RTP メディアストリームに、第三者の端末から、偽の音声やビデオの RTP メディアストリームが挿入・置換されることで、発信者が送ったメディアストリームとは異なるメディアが、受信者側で再生される。

また、RTP メディアデータを第三者が改ざんすることで、RTP メディアストリームの品質を低下させられたり、受信者側の再生が停止してしまう場合もある。

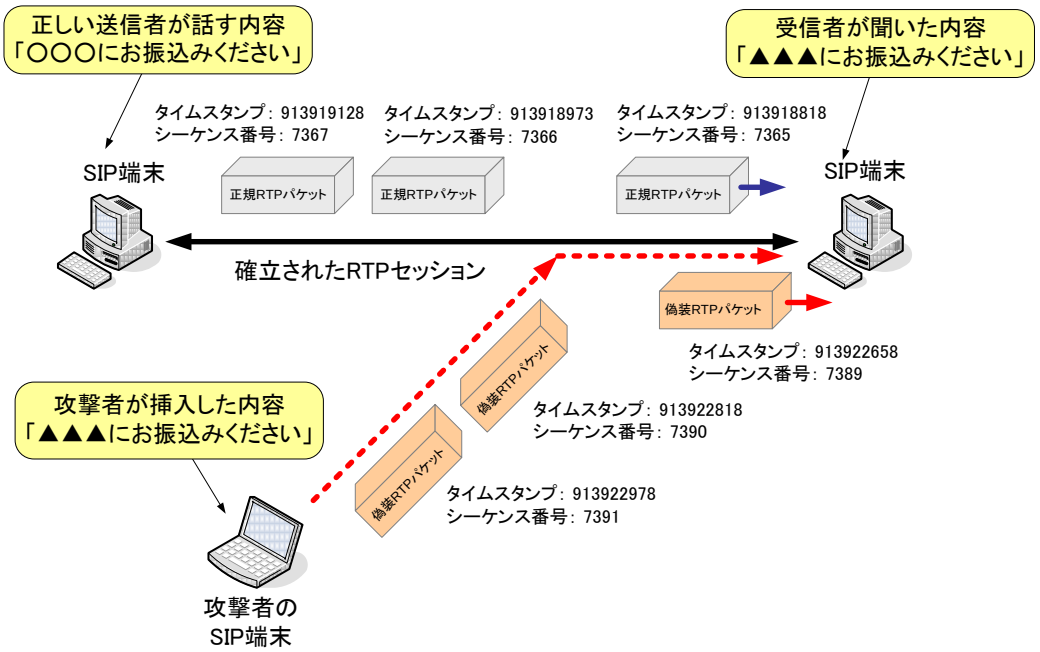


図 9-1　RTP メディアの挿入、ミキシングの構成

9.2　解説

【攻撃手法とその影響】

「図 9-1　RTP メディアの挿入、ミキシングの構成」はすでに確立された RTP セッション上の RTP メディアストリームに、攻撃者が偽装した RTP パケットを注入している状態を示す図である。真正な左の SIP 端末は、右の SIP 端末に対して RTP パケットでメディアストリームを転送している。このとき、攻撃者は真正な SIP 端末の RTP パケットのタイムスタンプとシーケンス番号をパケットキャプチャなどにより読み取り、そのタイムスタンプよりも大きい値のタイムスタンプを RTP パケットに書き込んで、右の受信 SIP 端末に注入する。また、シーケンス番号も、左の発信 SIP 端末が使っているシーケンス番号よりも大きい値を RTP パケットに設定する。

すると、受信端末は、タイムスタンプやシーケンス番号がより大きい値の RTP パケットを優先して処理して再生してしまう。

攻撃者はネットワーク上でパケットキャプチャを行い、すでに SIP によって確立された RTP メディアストリームを探す。その中から RTP メディアストリームを特定し、正しい発

【 項目 9. RTP メディアの偽装から起こる問題 】

信端末からのパケットであるかのように偽装した RTP パケットを、着信側端末に送信することで、着信端末に、本来の正しい発信側端末が送った音声やビデオとは異なるコンテンツを再生させる。

RTP メディアにはプッシュ番号(DTMF 信号)や端末機器の操作イベントを転送する機能もあるが、業界では特に VoIP 利用の普及を背景に、音声メディアの改ざんへの危険性を指摘する声が多い。

RTP 上の音声メディアストリームを改ざんする攻撃としては、RTP メディアストリームを転送するパケットのペイロードを、別の音声データに置き換えることで、まったく別の音声にしたり、元の音声に新しい音声をミキシング(合成)することで、背景音として別の声や音を混ぜたり、雑音を混入させて聞き取りにくくすることなどができる。

ライブ放送や、電話会議のような同報のメディアストリームの場合には、一部のメディアストリームが改ざんされると、一部の視聴者だけが別の音声を再生させられることになり、一種の「メディアハイジャック」状態になる。

この攻撃手法では、基本的には既存の RTP パケットをキャプチャして、コーデックにあわせて RTP のペイロードと一部ヘッダを書き換えるだけで済むため、事前の認証は不要である。また、一般的に、既存の IP 電話端末機器では、通信中に届く RTP パケットのタイムスタンプやシーケンス番号のズレが多少大きくても処理する傾向にあり、精密にタイミングを合わせる必要がないなど、攻撃難易度が必ずしも高いとは言えない。

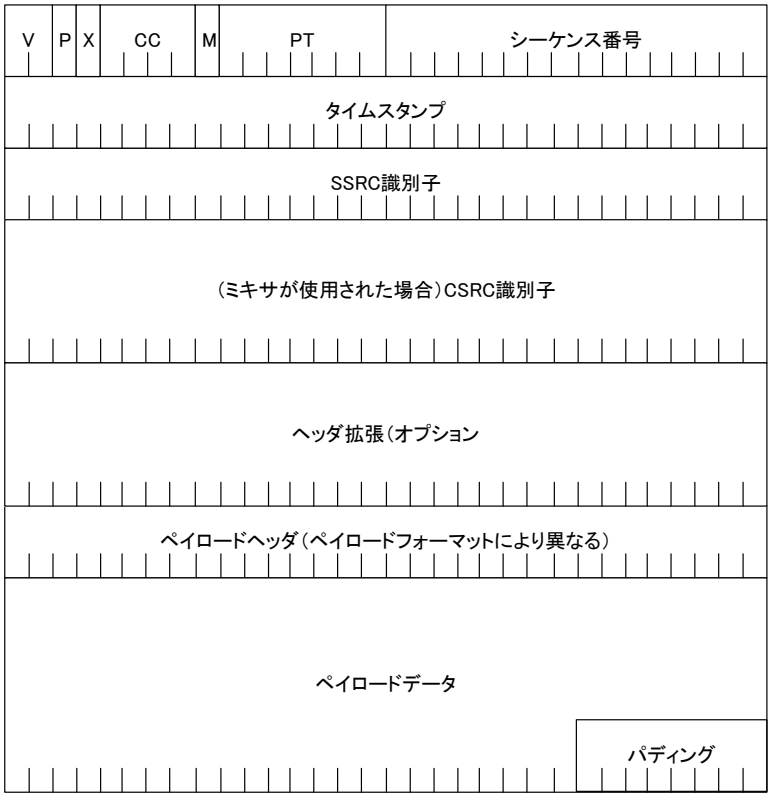


図 9-2 RTP のパケット形式

また、この手法は正しい発信者からの RTP パケットと、攻撃者が送信する RTP パケットの両方が、受信者端末に届くことになる。このときに攻撃者端末の RTP パケットが優先

【 項目 9. RTP メディアの偽装から起こる問題 】

的に処理されるようにするよう、攻撃者はより「新しい」メディアであるかのように見せるため、次のような方法がとられる。

1) 攻撃者が送信する RTP ヘッダのシーケンス番号が大きくなるよう書き換える
2) 攻撃者が送信する RTP ヘッダのタイムスタンプを加算して書き換える

RTP パケットの改ざん、なりすましの攻撃手法は、SIP/RTP の環境だけでなく、VoIP を利用するその他の環境にも同じように影響を与える。例えば H.323 や、MEGACO、Cisco の Skinny などの呼制御プロトコルを利用した IP 電話環境でも、音声などのメディアの転送には、共通して RTP が利用されているため、RTP メディアストリームの偽装が成立する。

【原因と考察】

一般的に、RTP メディアの偽装はむずかしいと考えられている。なぜなら、RTP パケットで伝送される音声やビデオは、再生タイミングを合わせるために、時刻に敏感であるためである。

しかし、RTP メディアストリームのパケットを受信した端末がメディアの再生処理をするとき、実は時間的なずれ(遅延)を検査しにくい、という背景がある。RTP パケットでは、音声・ビデオを、それぞれのコーデック(符号化・復号方式)を利用して、一定の間隔でデータとして転送するが、受信側では受け取るパケットの時間間隔は必ずしも一定の時間間隔にならない。例えば、端末の間にあるルータやスイッチのバッファの空き具合や、処理方法、経由する回線の速度の違いや、経路が異なるときのルータのホップ数などによっても、パケットが到達するまでの時間が異なる。また、パケットの到着順序が変わってしまったり、途中のネットワークで再送処理が行われて、同じ内容のパケットが重複して到着してしまうこともある。このような傾向が強く現れるのは、特に広域・大規模なネットワークを経由するときや、ケーブルや無線通信などの、多様な接続方法が含まれるときである。

このような IP パケットの転送上の不安定な振る舞いに対応するため、RTP を利用するソフトウェア上では「ジッタ・バッファ」と呼ばれる、遅延のばらつきを吸収するための一時蓄積用のメモリを用意している。ジッタとは、IP パケットが到着するまでの遅延のゆらぎのことである。「遅延がゆらぐ」というのは、例えば通常は 4ms の伝送遅延で到着するパケットが、あるときは 50ms もかかることがあることを指す。遅延がゆらぐことで、不意にパケット到着のタイムアウトが発生したり、パケットの順序入れ替えが起こったりする。こうしたパケットの伝送遅延を吸収するため、受信済みだけれども、まだ処理をしていない RTP パケットの内容をいくつかバッファに保持しておくことで、一部の RTP パケットの到着が多少遅れても、音とびなどが生じないように再生することができる。

このように、RTP を処理するソフトウェアは RTP メディアストリームのパケットの到着時刻のズレに対応する機能があるため、攻撃者によってなりすまされたパケットを受信して、真正なメディアストリームのパケットとして処理してしまう余地がある。

RTP メディアストリームが改ざんされる脅威については、RTP の RFC1889(1996 年 1 月) “9. Security”、”9.2 Authentication and Message Integrity”でも指摘されている。2003 年 7 月付けの更新版の RTP 標準である RFC3550 でも、RTP にはメッセージ認証の機能はなかった。

その後、RTP メディアストリームを保護するための SRTP が標準化され、SRTP を採用する製品もいくつか登場するようになった。しかし、SRTP のための安全な鍵交換の方法が標準化されていなかった。現在のところ、シグナリングを行う SIP を TLS か DTLS で保護しつつ、SRTP 用の共通鍵は SRTP メディアを確立する端末同士が別途、DTLS で鍵生成と交換を行う方向が有力である。

なお、RTP の保護方法に関する動向については「項目 8 RTP メディアの盗聴から起こる

問題」の「原因と考察」を参照していただきたい。

9.3 対策

【運用ガイド】

1) 偽装するホストが RTP を利用するネットワークに接続できないように、SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
2) IPsec、SSL-VPN などの暗号化トンネルを使って SIP/RTP 通信を保護する

【実装ガイド】

本脆弱性に対しては RTP パケットのなりすまし対策が必要である。

1) RTP メディアストリーム上で、SRTP のメッセージ認証機能を利用する

なお、SRTP でメッセージ認証機能を利用する場合も、メッセージ認証用の鍵が必要となるが、そのための鍵の交換方法がいくつか議論されているので「項目 8 - RTP メディアの盗聴から起こる問題 – 8.3 発見の経緯とトピック、対策の動き、現在の動向」をご参照いただきたい。

9.4 参考情報

公開年月	情報源
2006 年 12 月	“Hacking VoIP Exposed – Voice over IP Security Secrets & Solutions”, David Endler and Mark Collier; McGraw-Hill Professional Publishing; ISBN: 0072263644 http://www.hackingexposedvoip.com/
2007 年 5 月	Sipera への報告 Sipera - Unencrypted RTP vulnerable to capture and reconstruction http://www.sipera.com/index.php?action=resources,threat_advisory&tid=264& 暗号化していない RTP パケットは内容を再構成される恐れがあるという指摘。
2007 年 5 月	Sipera - RTP sequence number and timestamp can be guessed to inject media packets that may be accepted by receiver as legitimate http://www.sipera.com/index.php?action=resources,threat_advisory&tid=269& RTP シーケンス番号とタイムスタンプが予想され、正しい受信者が偽装されたメディアを受け入れてしまう、という指摘。
2007 年 3 月	Sipera - Rogue RTP injection may result in voice quality degradation http://www.sipera.com/index.php?action=resources,threat_advisory&tid=193& 悪意のある RTP パケットの挿入によって、音声品質が低下させられる問題の指摘。

【 項目 9. RTP メディアの偽装から起こる問題 】

9.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■Ⅰ（注意）	□Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値	2.6		

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響 （情報漏えいの可能性）	■なし	□部分的	□全面的
完全性への影響 （情報改ざんの可能性）	□なし	■部分的	□全面的
可用性への影響 （業務停止の可能性）	■なし	□部分的	□全面的

項目10. RTCP の偽装から起こる問題

10.1 概要

メディアストリームを転送する RTP に対して、RTP の制御を行う RTCP を偽装することで、特定の RTP メディアストリームを停止させたり、参加者名のなりすまし、より低品質なコーデックへのダウングレードが可能になる。

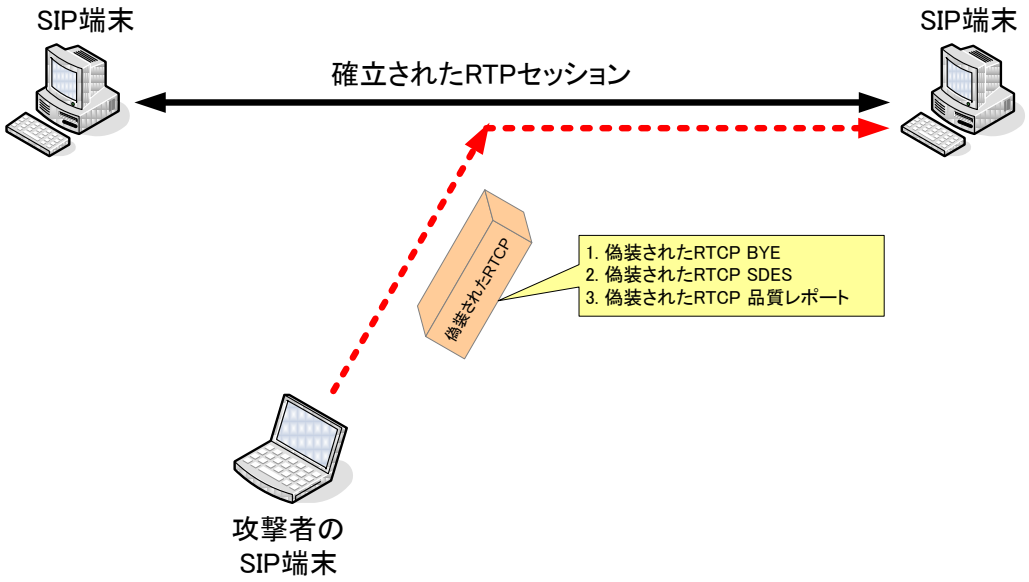


図 10-1 RTCP の偽装

10.2 解説

【攻撃手法とその影響】

メディアストリームの転送を行う RTP に対して、RTCP(RFC3550 – 6. RTP Control Protocol: RTP 制御プロトコル)は RTP の制御を行う、次のような機能がある。

1) 音声、ビデオなどのメディアソースの識別と、識別番号の自動的な衝突回避
2) 各メディアストリームを持つ参加者名の表示上の識別
3) メディアストリームの受信品質のレポート

この 3 つの機能について、RTCP の詳細に触れながら、既知の脆弱性として指摘されている内容を紹介する。

1) 偽装された RTCP BYE による RTP メディアの停止

すでに確立された RTP メディアストリームが、意図せず第三者から停止または中止させられる。第三者の端末から、特定の RTP ストリーム上のどれかの端末に、特定端末になりすまして RTCP の BYE メッセージを送り届けることで成立する。

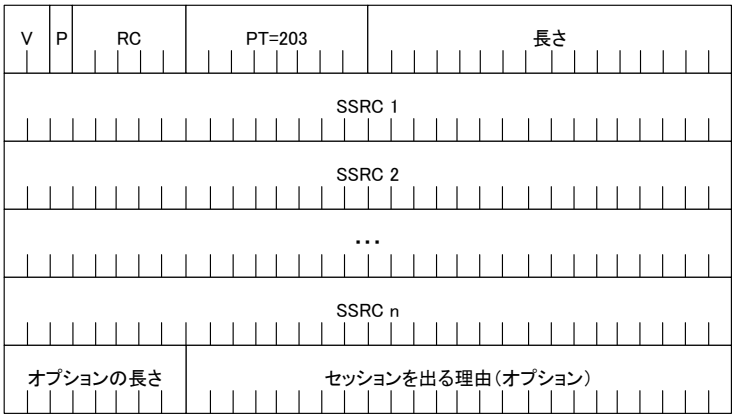
このとき、意図せず RTP ストリームが終了させられた端末またはサーバ上の、SIP レイヤのプロトコルスタック実装では、異なるプロトコル・コンポーネント間でのイベント通

【 項目 10. RTCP の偽装から起こる問題 】

知機構などがなければ、RTP ストリームの終了がわからない。SIP プロトコルや SIP 端末の制御部が RTP メディアストリームの終了がわからない場合、例えば通話は成立していて課金されているのに、音声だけが届かない、などの現象が起こる。

また、制御コンポーネントが RTP の終了を検出したとしても、偽装された RTCP BYE を受信した SIP 端末は「その参加者、またはメディアソースが離脱した」ということだけがわかるため、事実上の SIP セッションの終了や、音声・ビデオのメディアストリームの終了につながる。

これらの攻撃は SIP の認証とは関係なく実行できる。また、SIP を利用しない IP 電話システムでも、RTP を利用している IP 電話システムは多く、攻撃が成功する可能性がある。



V=バージョン番号
P=パディング
RC=SSRCヘッダの数
PT=パケットタイプ

図 10-2　RTCP BYE パケットのフォーマット

2)　偽装された RTCP SDES による発信者名のなりすまし

RTP メディアストリーム上で、RTCP を偽装して、参加者の発番号や発信者名を別の値に置き換え､詐称できることがある｡特定の RTP メディアストリーム上の端末のどれかに、偽装された RTCP のソース記述(SDES)パケットの NAME(表示名)、EMAIL(電子メールアドレス)、PHONE(電話番号)を送信する。RTCP SDES パケットを受信した RTP 端末は、これらの表示名、電子メールアドレス、電話番号などをそのまま受け入れてしまう場合がある。

また、RTCP SDES パケットは、1 つ以上の SSRC で示される RTP メディアストリームを、CNAME(Canonical Name)によってひとつの端末やセッションに対応づける役目を持つ。SSRC は音声やビデオのメディアストリームを識別する、一時的な値なのに対し、CNAME はユーザ名と端末の IP アドレスなどを使って一意になるように作られる､長期間にわたって使われる名前である。CNAME によって､「誰の」端末に「どのメディアストリームが対応する」というような対応付けができる。

しかし、RTCP パケットが暗号化やメッセージ認証などで保護されていないと、第三者に書き換えられることで予期しない結果となってしまう。

【 項目 10. RTCP の偽装から起こる問題 】

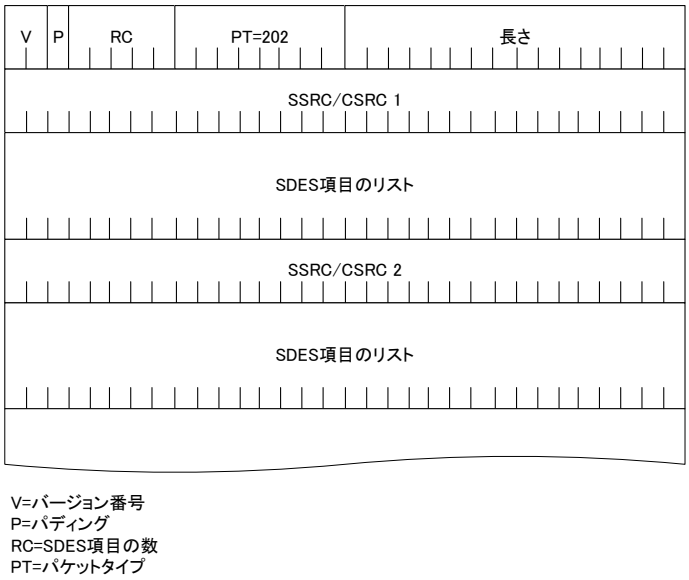


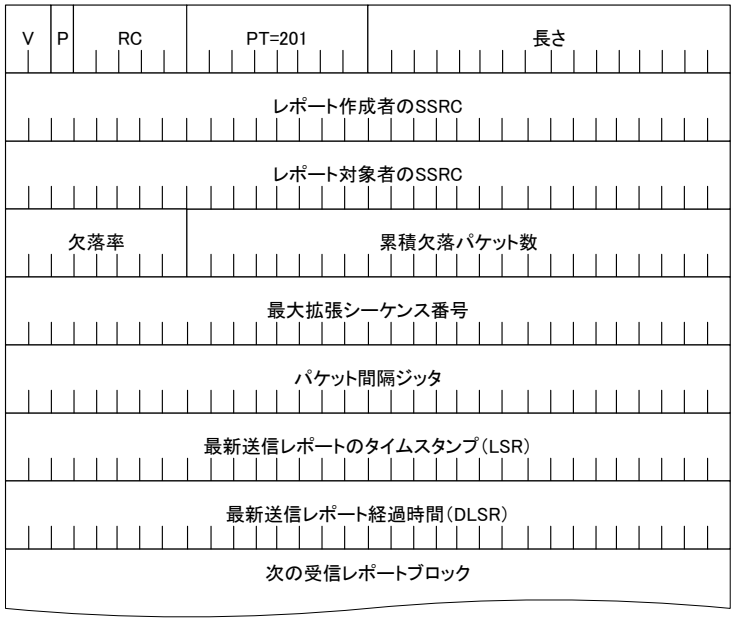
図 10-3 RTCP SDES パケットのフォーマット

3) 偽装された RTCP 品質レポートによる、低品質コーデックへのダウングレード

RTP メディアストリーム上で発生するパケット損失について、RTCP 受信報告(RR)パケットによって、パケット欠落率またはパケット欠落数を過大に報告されると、該当するメディアストリームに使われているコーデックが、より低品質のコーデックに変更させられることがある。

低品質のコーデックに変更させられることにより、通話中の音声品質が劣化して、相手の声や周囲の音が聞こえにくくなったり、テレビ電話の画像で相手の顔や状況が判別しにくくなるなどの影響がある。また、経由する回線品質が悪いとみなされて、通話やセッションそのものが終了してしまう場合もある。

【 項目 10. RTCP の偽装から起こる問題 】



V=バージョン番号
P=パディング
RC=受信レポートブロックの数
PT=パケットタイプ

図 10-4 RTCP 品質レポートのパケットフォーマット

【原因と考察】

1) 偽装された RTCP BYE による RTP メディアの停止

RTP では、音声やビデオなどのメディアストリームはそれぞれ SSRC という値で識別されている。SSRC は同期ソース識別子(Synchronization Source Identifier)の略で、目的は異なる音声とビデオを同期して再生するために、それぞれのメディアストリームを識別するために利用する。ここでいう同期とは、ビデオで表示される動画の動きと、音が再生されるタイミングが合っている、という意味である。例えば、しゃべっている人の動画に映る口の動きと、話している声のタイミングを合わせるなどである。

SSRC に話を戻す。SSRC は RTP メディアストリームごとに、おのおのの SIP/RTP 端末上で動的に生成される識別子である。32bit 長があるが、生成方法やタイミングによっては異なる端末上で生成される SSRC の値が同じになり、値が衝突することもある。このようなときに、SSRC の値の衝突を検知した SIP/RTP 端末は、値が衝突している SSRC を指定して RTCP BYE を送り、自分が使おうとしていた SSRC を RTP メディアストリームから離脱させることができる※。

※ RTP - 8.2 Collision Resolution and Loop Detection, RFC3550
http://tools.ietf.org/html/rfc3550#section-8.2

また、RTCP BYE を受信した SIP/RTP 端末は、RTCP BYE の中で指定された SSRC はメディアストリームから離脱したとみなし、その SSRC を持つ RTP パケットは受け付けなくなる。

RTCP BYE パケットに必要な情報は、離脱させる SIP/RTP 端末の RTP メディアストリームのソース識別子(SSRC)で、既存の RTP メディアストリームをパケットキャプチャすることで得られる。RTCP BYE パケットには、シーケンス番号もタイムスタンプも不要な

【 項目 10. RTCP の偽装から起こる問題 】

め、RTP メディアの偽装よりも簡単に偽装パケットを作ることができる。

2) 偽装された RTCP SDES による発信者名のなりすまし

RTCP ソース記述(SDES)パケットは、1 台の SIP/RTP 端末や、1 セットの SIP/RTP ソフトなど、SIP/RTP のセッションの参加者と、その参加者が利用する 1 つ以上の RTP メディアストリームを対応づける役割を持つ。RTCP ソース記述パケットの必須項目にある CNAME(Canonical Name: 標準名)は、RTP メディアストリームにつけられる一時的な値である SSRC を 1 つ以上まとめて、ユーザ名のような形でまとめて名前付けしておくのに使われる。RTP 上では、CNAME を基点とした、メディアストリームの束があるようなイメージになる。

RTCP SDES パケットでは、CNAME のほかに、表示名や電話番号、位置情報なども転送できるが、RTCP 自体にはメッセージ認証などのメカニズムがないため、これらの情報は相手ユーザが任意に設定できるほか、第三者からの改ざんも受け入れてしまうことになる。RTCP SDES パケットも、RTCP BYE と同様に、シーケンス番号もタイムスタンプもないため、偽装パケットを作るには、SSRC があればよい。

3) 偽装された RTCP 品質レポートによる、低品質コーデックへのダウングレード

RTCP の受信品質レポート(RTCP RR)は、さまざまな環境で RTP 上のメディアストリームが適切な品質で符号化されるよう、自律的に適応するための重要な機能である。RTCP RR には以下のような情報がある。

① レポート作成者の SSRC
② レポート対象者の SSRC
③ 累積欠落パケット数
④ 最大拡張シーケンス番号
⑤ 欠落率
⑥ パケット到着間隔ジッタ

このうち、正しい受信レポートになりすまして、送信端末に対して累積欠落パケット数、欠落率を過大に報告することにより、送信端末はより耐性の高い、しかし品質の低いコーデックを選択して切り替える場合がある。例えば、G.711 のような 64Kbps の PCM 音声符号化方式を利用していた RTP メディアストリームに、過大な欠落率を報告することで、より強固な誤り訂正機能を持つ冗長符号を追加させ、その代わりに音声の符号化データは少なくなっていく、という結果である。通常、IP 電話端末は最低で 4～8Kbps 程度の高い圧縮率を持つ音声符号化方式も実装していることが多いため、低品質なネットワーク環境では、こうした低レートの符号化方式が選択されることも考えられる。しかし、4～8Kbps では、一般には人の話を単語単位では理解できるが、数字や記号を伝えようとすると難しいことがある。また、このような低レートの符号圧縮技術では、人間の声帯の発声方法に最適化された圧縮を行っているため、音楽や背景音などは聞き取れない。

このような低品質化を利用して、偽の通話者を特定しにくくすることも考えられる。

4) RTP がセッション制御機能を持っている背景

RTCP による RTP の制御機能については疑問もある。本来、セッションの制御を行う「シグナリング機能」は SIP が担当しているはずなのに、なぜ、メディア機能を担当している

【 項目 10. RTCP の偽装から起こる問題 】

RTP が独自に停止やコーデックの変更などのシグナリングを勝手に行ってしまうのか？という疑問である。これには、RTP の過去の成り立ちが関係している。

RTP はもともと、H.323 や MEGACO のような、初期段階の IP 電話の時代からメディアデータの転送に利用されていた。特に MEGACO は既存のアナログ電話機をそのまま IP 化するプロトコルで、SIP のような高機能な呼制御プロトコルを利用していなかった。また、電話会議のような高度な利用方法では、H.323 の呼制御プロトコルでも、完全に RTP の制御には対応していなかった。そのため、一部の呼制御機能を RTP に持たせる必要があった。

現在は SIP 端末ごとの RTP セッションと RTP のメディアストリームの対応付けは SIP が行う形になっており、SDP が利用できる。また、参加ユーザの表示名やメールアドレス、位置情報、ステータスなどは SIP のプレゼンス機能を利用することができる。

ただし、RTP は自律的に回線品質に適応するために必要な、RTP の受信品質レポート機能は RTCP 以外に代替がない。また、SSRC(同期ソース記述子)の衝突回避のための RTCP BYE も他の代替策が見当たらない。この 2 つの機能に依存する限り、RTCP は SRTP などでの保護が必要となっている。

10.3 対策

【運用ガイド】

1) 偽装するホストが RTCP を利用するネットワークに接続できないように、SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
2) 偽装された RTCP パケットが注入されないよう、IPsec、SSL-VPN などの暗号化トンネルを使って SIP/RTP 通信を保護する。

【実装ガイド】

1) RTCP を SRTCP で保護する

なお、SRTP でメッセージ認証機能を利用する場合も、メッセージ認証用の鍵が必要となるが、そのための鍵の交換方法がいくつか議論されているので「項目 8 - RTP メディアの盗聴から起こる問題 – 8.2 原因と対策」をご参照いただきたい。

【 項目 10. RTCP の偽装から起こる問題 】

10.4 参考情報

公開年月	情報源
1996 年 1 月	RFC1889 - RTP: A Transport Protocol for Real-Time Applications (廃止) http://www.networksorcery.com/enp/rfc/rfc1889.txt
2002 年	@STAKE Inc., VoIP – The Next Generation of Phreaking http://www.blackhat.com/presentations/win-usa-02/arkin-winsec02.ppt RTP も含めた脆弱性を幅広く指摘したプレゼン資料。
2003 年 7 月	RFC3550 – RTP: A Transport Protocol for Real-Time Applications 6. RTP Control Protocol (RTCP) http://tools.ietf.org/html/rfc3550#section-6 8.2 Collision Resolution and Loop Detection http://tools.ietf.org/html/rfc3550#section-8.2
2003 年 7 月	RFC3551 - RTP Profile for Audio and Video Conferences with Minimal Control http://tools.ietf.org/html/rfc3551
2004 年 4 月	「マスタリング TCP/IP RTP 編」Colin Perkins 著、小川 晃通 監訳、オーム社、2004 年 4 月、ISBN:27406561
2005 年 8 月	NEC Network Laboratories, “VoIP Security Threat Analysis” P.8, RTP/RTCP-specific DoS attacks http://www.ibr.cs.tu-bs.de/projects/nmrg/meetings/2005/nancy/voip-sec.pdf RTCP BYE を利用した DoS、RTCP RR を利用したダウングレード攻撃の指摘。
2007 年 3 月	I-D - VoIP Security Threats relevant to SPEERMINT (期限切れ) 2.4. Threats to MF Availability http://tools.ietf.org/html/draft-niccolini-speermint-voipthreats#section-2.4 SIP/RTP に関する問題点の整理とベストプラクティス(BCP:次善の策)。ドラフト 05 の時点では、すべての対策案が整理されてはいないのが現状。
2009 年 5 月	I-D - SPEERMINT Security Threats and Suggested Countermeasures (最新) 2.4. Threats to the Media Function (MF) http://tools.ietf.org/html/draft-ietf-speermint-voipthreats#section-2.4 I-D - VoIP Security Threats relevant to SPEERMINT の最新ドラフト。ドラフト 04 の時点では、すべての対策案の整理はされていない。

【 項目 10. RTCP の偽装から起こる問題 】

10.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■Ⅰ（注意）	□Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値	2.6		

※本評価は、深刻度の最も高い「偽装された RTCP BYE による RTP メディアの停止」を対象としたものである

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響 （情報漏えいの可能性）	■なし	□部分的	□全面的
完全性への影響 （情報改ざんの可能性）	■なし	□部分的	□全面的
可用性への影響 （業務停止の可能性）	□なし	■部分的	□全面的

【 項目 11. コーデックの脆弱性 】

項目11. コーデックの脆弱性

11.1 概要

本資料の執筆時点では、音声、画像、動画の符号化方式、データ形式などのコーデック(CODEC)そのものの脆弱性は、SIP/RTP 関連の書籍や Web 上の情報に見当たらなかった。

なお、コーデックを利用するソフトウェア製品やソフトウェアライブラリの実装上の不具合や、ソフトウェアが不具合を起こしやすいデータの問題については「項目 12 不具合を起こしやすいパケットに対応できない問題」を参照してほしい。

【 項目 12. 不具合を起こしやすいパケットに対応できない問題 】

項目12. 不具合を起こしやすいパケットに対応できない問題

12.1 概要

不具合を起こしやすいパケットを受け取ると、SIP/RTP 対応機器やソフトウェアの機能が停止、再起動したり、予想以上に処理時間がかかることがある。場合によっては機器の制御を奪われ、乗っ取られた SIP/RTP 対応機器が攻撃者から自在に操られ、第三者に危害を加えることもある。

12.2 解説

【攻撃手法とその影響】

不具合を起こしやすいパケットとは、標準仕様に違反した長すぎる文字列や、仕様で決められた範囲の境界の前後にある数値などを含むパケットのことを指す。攻撃者はこのようなパケットを対象の SIP 端末などに送信すると、パケットを受信した SIP 端末が停止したり、再起動したり、動作が遅くなり、結果的にサービス不能攻撃(DoS)が成立することがある。この攻撃手法では、脆弱性の問題を誘発するようなメッセージを含む、ある 1 つのパケットを送信するだけで攻撃が成功してしまう点に大きな問題がある。

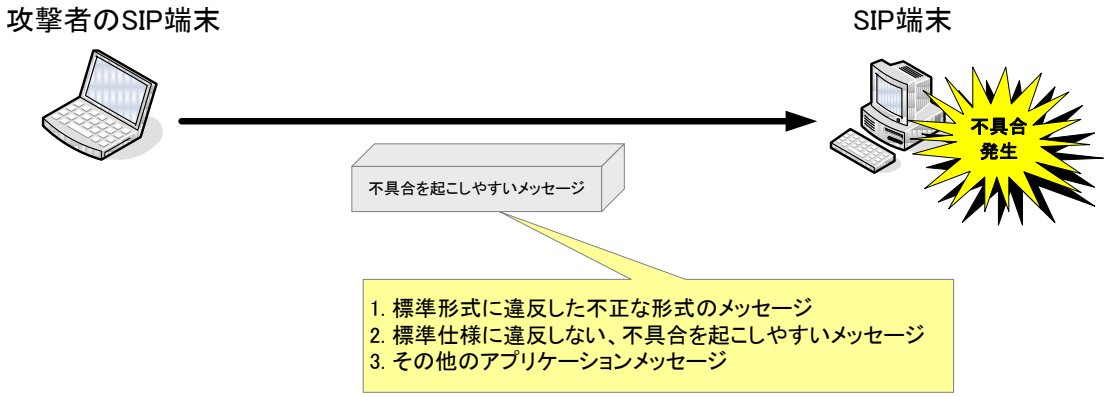


図 12-1 不具合を起こしやすいパケットの送信による攻撃

1) 標準仕様に違反した不正な形式のパケット

標準仕様に違反したパケットにはさまざまなものがある。文字列として表現すべきフィールドが、ASCII 文字ではないバイナリで表現されていたり、1 行の文字列が数千文字以上に渡るもの、正の整数を書くべきフィールドにマイナスの数値がある、などである。図 12-2 は、不具合を起こしやすいパケットの内容例として、標準にはない SIP メソッド名で、予想以上に長い文字列 SIP メソッド名が、1 行目のリクエストラインに書かれている、SIP リクエストメッセージの例を示している。

【 項目 12. 不具合を起こしやすいパケットに対応できない問題 】

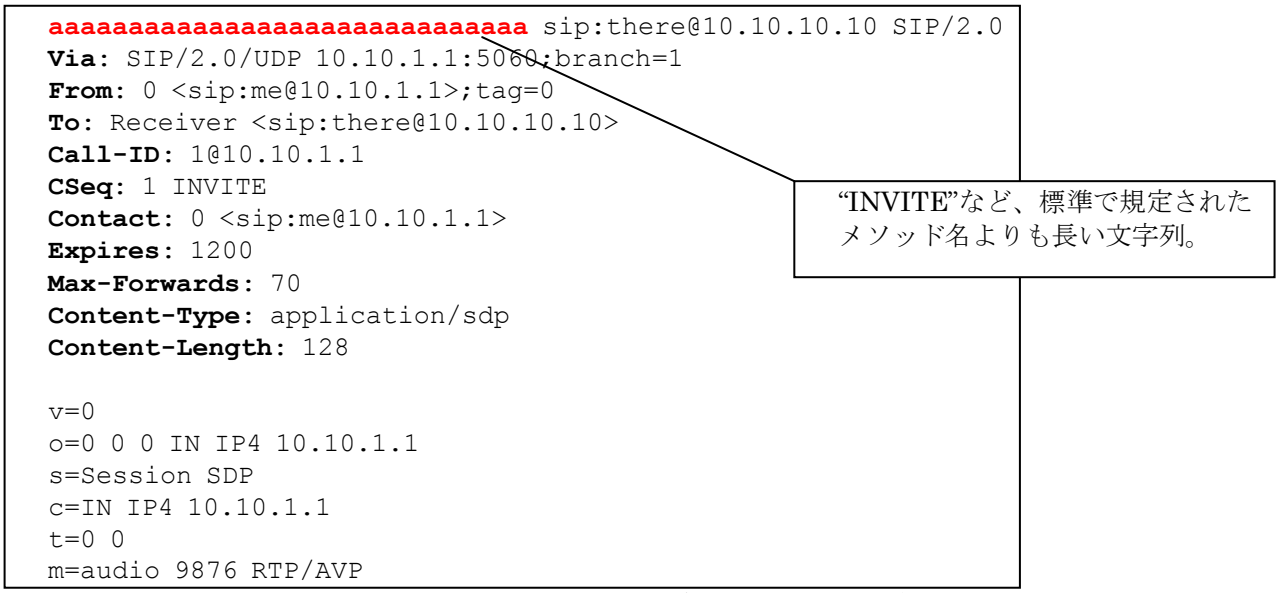


図 12-2. 標準にない、長い SIP メソッド文字列がかかれたメッセージの例

こうした不正形式メッセージを含むパケットが SIP/RTP 対応機器の不具合を誘発すると、機器の機能が停止して利用できなくなったり、機器が再起動して、それまで利用していたセッションが消滅したりする。機器の動作が遅くなると、音声のとぎれが発生したり、認証が成功したりしなかったりするなど、動作が不安定になる。

また、不正な形式のメッセージを含むパケットによる不具合は、機器のソフトウェア上の制御を奪う攻撃にも利用される。例えば、大量の文字列を受信したときに不具合を起こす機器は、ソフトウェア的にはバッファオーバフローを発生させている可能性が高い。攻撃者はバッファオーバフローを利用して、侵入用の実行コードを、機器内部のメモリ上に展開することで、攻撃者は機器のソフトウェア上の制御を奪うことができる。

制御を奪われた機器は、さらに別の実行プログラムを注入されるなどして、他の端末を攻撃させられる。さらに、攻撃者は乗っ取った複数の端末を同時に利用して、ウイルスが添付された攻撃メールの送信や、別のサイトへの分散 DoS 攻撃を行うこともある。攻撃者によって遠隔制御用のプログラムをインストールされて制御を奪われ、攻撃者に操られているコンピュータを「ボット」と呼び、複数のボットが特定の攻撃者によって操作される構造を「ボットネット」などと呼ぶ。2007 年 7 月現在、SIP/RTP 関連機器がボットネットに組み入れられた、という報告事例は見当たらないが、組込機器への脅威として可能性が指摘されている [Hacktool.Sipbot]。

不正形式のメッセージを含むパケットを送り込む攻撃手法は”Fuzzing”(ぼかした、あいまいな、の意味)とも呼ばれ、特に動作するプログラムの不具合を誘発することを目的にしている。また、Fuzzing の研究分野では、不具合を誘発するようなデータの値や形式をいかに広範囲に、自動生成するかがテーマとなっていて、いくつかのツールが開発され、利用されている。

【 項目 12. 不具合を起こしやすいパケットに対応できない問題 】

2) 標準仕様に違反しない、不具合を起こしやすいパケット

```
INVITE sip:sips%3Auser%40example.com@example.net SIP/2.0
To: sip:%75se%72@example.com
From: <sip:I%20have%20spaces@example.net>;tag=938
Max-Forwards: 87
i: esc01.239409asdfakjkn23onasd0-3234
CSeq: 234234 INVITE
Via: SIP/2.0/UDP host5.example.net;branch=z9hG4bKkdjuw
C: application/sdp
Contact:<sip:cal%6Cer@host5.example.net;%6C%72;n%61me=v%61lue%25%34%31
>
Content-Length: 150

v=0
o=mhandley 29739 7272939 IN IP4 192.0.2.1
s=-
c=IN IP4 192.0.2.1
t=0 0
m=audio 49217 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC
```

図 12-3. %XX の形式で一部の文字がエスケープされたメッセージの例（RFC4475）

図 12-3 は RFC4475 “SIP 拷問テスト”に含まれているテストの一例で、SIP メッセージの一部の文字を%記号に続けて 2 文字の 16 進数でエスケープ表現したものである。このメッセージは SIP の標準仕様に背反はしていないが、実装によっては処理できなかったり、予期しない不具合を起こしてしまう場合がある。そのため、このような、不具合を誘発するメッセージを含むパケットを 1 つ送るだけで、対象の製品に不具合を起こさせることができる。

標準仕様には違反しないが、不具合を起こしやすいメッセージには、例えば次のようなものがある。

① ある決められた範囲の境界の前後にある値を使う、入力されたとき
② エスケープ文字など、例外的な扱いの表現、データ形式を扱うとき
③ 同じセッション終了、同じオブジェクト消去が 2 回以上連続するようなメッセージ
④ 認証が必要な場面で、認証手順を経ていないメッセージ
⑤ ある条件では「届かないはず」のメッセージが届くとき
⑥ 意図的に復号に時間がかかるようなビット列(コーデック)
⑦ 長い文字列
⑧ セパレータ文字の繰り返し (“;”や”,”など)

全体をまとめると、通常の正しい形式の境界にあるメッセージや、正常な手順ではない例外的な状態が該当する。このような状態は、必ずしも悪意を持った攻撃者によるものだけではなく、無線のようにパケットロスしやすい状況での再送や、携帯型端末の電源復帰状態からの処理の不整合など、さまざまな要因で発生する可能性があるとも言える。

不具合を起こしてしまう機器やソフトは、結果として、機能が停止したり、再起動したり、処理に時間がかかるようになることがある。また、認証を回避された場合は、第三者によるなりすましの不正利用や、利用した料金を他のユーザにおしつける、などの不正利用を誘発する可能性がある。

【 項目 12. 不具合を起こしやすいパケットに対応できない問題 】

3) その他のアプリケーションメッセージ

不具合を起こしやすいメッセージには、他のアプリケーションとの間での想定外の利用方法にあたるものもある。例えば、番号やユーザ名を SQL データベースで検索するシステムがあるときに、ユーザ名として与えられた文字列に SQL の命令を実行させるコードが含まれており、そのまま実行してしまう、などである。SQL インジェクションと呼ばれる、この手法を利用すると、認証が必要な場面で特権ユーザとして認証させたり、データベース内部を破壊することも可能になる。

このような、複数の機能が連携するときの脆弱性については Web アプリケーションの脆弱性が多数報告されており、SIP/RTP 関連機器にも同様の危険があると考えられる。SIP/RTP 関連機器の場合、SIP/RTP そのものの機能以外にも、認証・課金機能や管理機能、監視機能などに HTTP や SQL などの異なる機能が多数利用されており、注意が必要だ。なお、SIP/RTP 関連機器がよく利用する管理機能の問題については「項目 18 管理機能の問題」に整理してあるので参照してほしい。

【原因と考察】

1) 標準仕様に違反した不正な形式のメッセージ

不正な形式のメッセージを使った攻撃は簡単に実行できるため、今でも IP ネットワークのインフラには日常的に不正な形式のパケットが到着している。現在はさまざまなアプリケーションに向けた不正メッセージが送信されており、SIP/RTP 関連機器も十分な対策が必要である。

不正な形式のメッセージによって、機器が不具合を起こす原因は、ソフトウェアの実装にある。特にコーディング時に適切に文字列を扱っていない、整数を型どおりに適切に処理していない、バッファメモリを保護していないなどの実装により発生する。さらに、文字列型のデータは SIP メッセージ全般に用いられており、正確な処理が必要である。よくある文字列の操作ミスとしては、C 言語でのメモリコピーや、`strcpy()` や `gets()` などの脆弱性を持つ文字列関数を利用して、関数の戻りアドレスなどを上書きしてしまう例である。また、整数については、型によって異なる整数の値の範囲を超えて加算したり、型変換を行うことで、予想外のメモリ領域をアクセスしてしまう例などがある。

こうした、コンピュータ言語を使ってコーディングをする過程で、脆弱性を作りやすい問題点は「セキュアコーディング」というキーワードで指摘されている。特に「C/C++セキュアコーディング」には、C 言語と C++言語を使う上での脆弱性の落とし穴と原理が詳しく説明されている。現在の SIP/RTP 関連機器は C/C++言語を利用した実装がほとんどと考えられるため、C/C++言語に特有のコーディング上の問題を理解することは重要である。

不正な形式のメッセージを送信する、この攻撃手法はコンピュータのソフトウェアに共通の問題であるため、SIP 関連プロトコルに限らず、広範囲にわたるソフトウェアに内在していると考えられている。例えば、不正な形式のメッセージを送信することによって、ソフトウェアの機能が停止したり暴走を起こす脆弱性は、SIP/RTP を利用した、製品の中心になるソフトウェアのほか、機器の管理機能を提供する、HTTP や SNMP、TELNET、RLOGIN、TFTP、NTP、DHCP、DNS などのソフトウェアにも含まれている。

2) 標準仕様に適合するが、不具合を起こしやすいメッセージ

標準仕様の範囲内で不具合を起こしやすいメッセージは、本来は SIP 関連プロトコルを利用する機器の開発過程でテストされているべきであるとも言える。しかし、日々拡張される SIP プロトコルの機能を実装することに追われて、セッションの状態に合わせた適切なメッセージ処理が実装できていないこともあるし、SIP プロトコルが拡張される過程で、

【 項目 12. 不具合を起こしやすいパケットに対応できない問題 】

実装条件が明らかになっていないこともある。
よくある事例としては%、などのエスケープ文字の処理が適切に行われていない場合がある。
現在のところ、SIP 関連プロトコルを利用した機器に対する攻撃事例として、標準仕様の範囲内での事例はほとんど報告されていない。その理由は、不正な形式のメッセージを使った攻撃のほうがはるかに簡単であるからだ。しかし今後、不正な形式のメッセージに対応できない脆弱性が解消されると、攻撃の手法を探す攻撃者が、よりハイレベルの標準仕様に適合した、攻撃メッセージを使うようになる可能性がある。
SIP/RTP のメッセージはそれぞれ RFC で標準化されているが、実際のプログラムは常に正しい形式のメッセージを送信するとは限らない。さまざまな要因によって、標準仕様とは異なるメッセージが届くことがある。その一例をあげてみよう。

① 設定の間違いで、まったく異なるプロトコルのパケットが届くことがある
② 受信したメッセージが何かの都合で一部が欠けていたり、書き換わっていることがある
③ 送信者の実装の不具合で、受信したメッセージの行や値が欠けていたり、長すぎることがある
④ 送信側端末の利用手順の都合で、メッセージが連続して届くことがある
⑤ 送信側端末の接続状態の変化とソフトウェアの状態不一致のため、未認証のリクエストや、本来あるべきではないリクエストやレスポンスが届くことがある

また、標準仕様に適合したメッセージであっても、SIP で定義されていない順序で SIP メッセージを受信することもある。このような順序や状態に無関係なメッセージを受信したときに、適切に無視をしたり、再送をするなど、適切な処理を行うことが必要である。

12.3 対策

【運用ガイド】

1) 製品の脆弱性が発見された場合は、製品開発元から提供されるソフトウェアの更新等を適用する。
2) 導入前に製品の導入ガイド、安全対策ガイド等の資料をよく理解して、これに従う。
3) ソフトウェアの更新が提供されない場合は、脆弱性を持つ機器が収容されるネットワークへのアクセス制限をして、攻撃しにくくする。
4) SIP/RTP の Fuzzing 攻撃を検出/防御するような、IDS/ファイアウォールを追加する方法もある。

【実装ガイド】

1) 企画・設計、コーディング、出荷のすべての開発生産過程を通して、脆弱性を混入させないための対策が必要である。特に出荷前の脆弱性対策が重要である。
2) 出荷後の問題に対応するために、製品にソフトウェアの更新機能を搭載することも有用である。
3) 排除しきれない脆弱性がある場合は、導入ガイド、安全対策ガイドなどの資料も提供すること。

【 項目 12. 不具合を起こしやすいパケットに対応できない問題 】

12.4 参考情報

公開年月	情報源
1999 年	CVE – Common Vulnerabilities Exposures http://www.mitre.org/
2003 年 2 月	JVN – Japan Vulnerability Notes: 日本脆弱性レポート(日本語) http://jvn.jp/
2003 年	Security testing of SIP implementations Christian Wieser, Marko Laakso Department of Electrical and Information Engineering University of Oulu http://www.mediateam.oulu.fi/publications/pdf/462.pdf PROTOS c07-SIP に関する Oulu 大学の論文
2006 年 3 月	Sipera への報告 Sipera - Comprehensive VoIP Security for the Enterprise: Not Just Encryption and Authentication http://www.sipera.com/assets/Documents/whitepapers/Sipera_Enterprise_VoIP_Security_WP.pdf
2006 年 5 月	RFC4475 - Session Initiation Protocol (SIP) Torture Test Messages http://tools.ietf.org/html/rfc4475
2007 年	IPA セキュア・プログラミング講座 http://www.ipa.go.jp/security/awareness/vendor/programmingv2/
2007 年 7 月	IPA セキュリティエンジニアリング - ソフトウェア開発者向けのページ 1. セキュリティ脆弱性の低減 http://www.ipa.go.jp/security/awareness/vendor/software.html#1
2005 年 6 月	「脅威モデル」Frank Swiderski、Windows Snyder 著、渡部 洋子 監訳、日経 BP ソフトプレス、2005 年 6 月、ISBN:4891004576
2005 年 1 月	PROTOS Test-Suite (c07-sip) - Security Testing of Protocol Implementations http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/
2006 年 11 月	「C/C++セキュアコーディング」Robert C. Seacord 著、歌代和正 監訳、JPCERT コーディネーションセンター訳
2007 年 5 月	Symantec Security Response - Hacktool.Sipbot http://www.symantec.com/security_response/writeup.jsp?docid=2007-050914-5546-99&tabid=2 ボットネットによる SIP インフラへの攻撃のコンセプトを実証するツール(Java)。
2008 年 8 月	VoIP Security - Threats and Countermeasures http://www.apan.net/meetings/newzealand2008/presentations/sip/apan26-eric.pdf SIP ベースの IP 電話システムから見たセキュリティの概要。
2008 年 2 月	Exposing Vulnerabilities in Media Software http://www.blackhat.com/presentations/bh-europe-08/Thiel/Whitepaper/bh-eu-08-thiel-WP.pdf iSEC PARTNERS 社の BlackHat 2008 での発表資料。 Ogg、Speex、FLAC、MPEG4 を利用した実装への Fuzzing の可能性を示す
2008 年 2 月	RFC5118 - Session Initiation Protocol (SIP) Torture Test Messages for Internet Protocol Version 6 (IPv6) http://tools.ietf.org/html/rfc5118

【 項目 12. 不具合を起こしやすいパケットに対応できない問題 】

2008 年 9 月	SIP スタックの実装の未熟さを突く攻撃(後編) http://itpro.nikkeibp.co.jp/article/COLUMN/20080926/315503/ 日本製 SIP 脆弱性検査ツールを開発・販売する NextGen ネットワークセキュリティ事業本部長による日本語の解説

12.5 CVSS 深刻度評価(参考値)

【評価結果】バッファオーバフローの場合

本脆弱性の深刻度	□ Ⅰ （注意）	□ Ⅱ （警告）	■ Ⅲ （危険）
本脆弱性の CVSS 基本値			7.5

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	□高	□中	■低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響 （情報漏えいの可能性）	□なし	■部分的	□全面的
完全性への影響 （情報改ざんの可能性）	□なし	■部分的	□全面的
可用性への影響 （業務停止の可能性）	□なし	■部分的	□全面的

【 項目 13. Call-ID を予測しやすい実装の問題 】

項目13. Call-ID を予測しやすい実装の問題

13.1 概要

MAC アドレスを含む乱数性が低い値が使われるなど、Call-ID が予想されやすい実装が存在する。

13.2 解説

【攻撃手法とその影響】

SIP 端末が登録に使用する REGISTER リクエストの Call-ID を予想して REGISTER リクエストを偽装することにより、SIP サーバに記録されている CSeq 値を不当に増加させ、正規の登録リクエストを受信しても、サーバが拒否してしまう可能性がある。

【原因と考察】

RFC3261 の 8.1.1.4 Call-ID　には以下のようにある。

「暗号的にランダムな識別子の使用は、セッションの乗っ取りに対するある種の防御を提供し、起こりうる意図しない Call-ID の衝突を減らす。」

INVITE など From ヘッダや To ヘッダの tag 値と合わせて同一性をチェックする場合にも攻撃の難易度が下がってしまうが、もっとも影響があると考えられるのは REGISTER リクエストである。REGISTER リクエストは、SIP 端末をサーバに登録する際に使用されるが、SIP 端末が連続して起動している間は同じ Call-ID が使用されるべきとされている。予測された Call-ID を使った REGISTER リクエストが、本物の REGISTER リクエストと衝突した場合、認証による確認が行われたとしても、サーバが Call-ID と関連付けて記憶する CSeq 値は増加させられてしまう可能性がある。CSeq 値は同じ端末間で複数のリクエストを送受信し合うときに、連続して受信したリクエストの生成された順番を確認できるようにつけられる値である。新しいリクエストを処理した後に、古いリクエストを処理してしまうと、端末間で共有している状態が食い違うなどの問題が起こるため、古いリクエストは破棄されてしまう。もしも、攻撃により端末が管理している CSeq が増加してしまうと、正規の登録リクエストを受信しても、Cseq 値が小さいためサーバが拒否してしまう。

【 項目 13. Call-ID を予測しやすい実装の問題 】

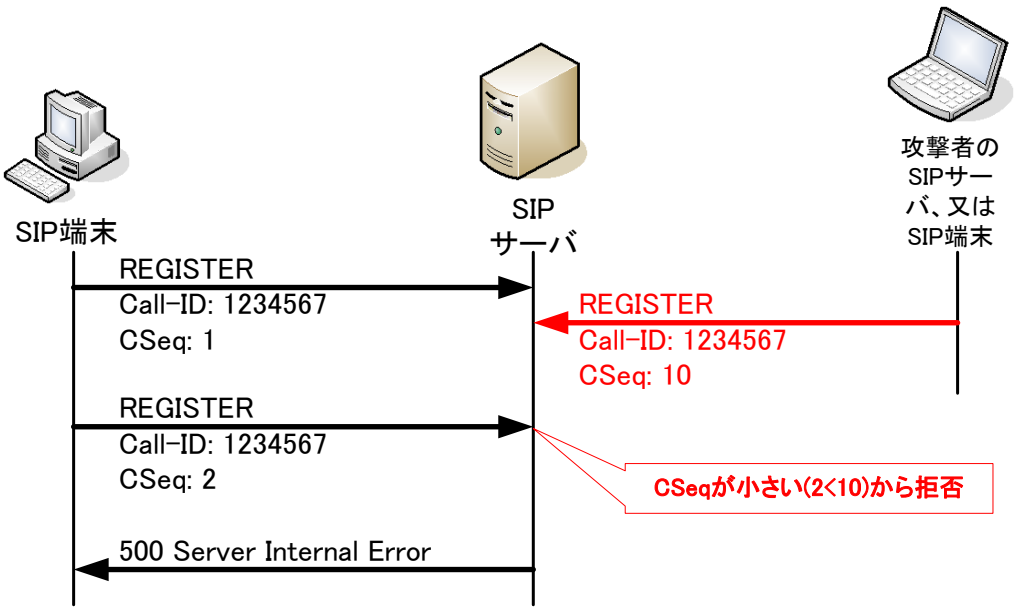


図 13-1 Call-ID が衝突した場合の Cseq への影響

13.3 対策

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【実装ガイド】

1) RFC の仕様に沿って実装する
   根本的には、予測されないように乱数性を確保して Call-ID を生成する
2) CSeq 増加のチェック
   認証が必要とされている場合は、認証されていないリクエストによる CSeq の増加を一時的に保留する

13.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol 8.1.1.4 Call-ID http://tools.ietf.org/html/rfc3261#section-8.1.1.4 8.1.1.5 CSeq http://tools.ietf.org/html/rfc3261#section-8.1.1.5
2006 年 7 月	SIP Stack Fingerprinting and Stack Difference Attacks http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Scholz.pdf

【 項目 13. Call-ID を予測しやすい実装の問題 】

13.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	□ Ⅰ（注意）	■ Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値		4.0	

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	■なし	□部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

項目14. 認証機能の不十分な実装の問題

14.1 概要

認証動作が不完全で、認証時の検証作業が不十分であったり、認証後のパラメータの維持や照合動作の不足により、認証が済んでいない第三者の端末からのなりすましメッセージを受け入れてしまうことがある。

14.2 解説

【攻撃手法とその影響】

不正にキャプチャして取得した SIP リクエストに記述されている、認証ヘッダをコピーして、偽装リクエストを作成することにより、チェックの甘いサーバ・端末の認証チェックを通ってしまい、偽装リクエストが処理されてしまう。または、不正に解読された認証のパスワードを使い、ランダムに作成された nonce, opaque などのパラメータから認証ヘッダを生成して偽装リクエストを作成する。

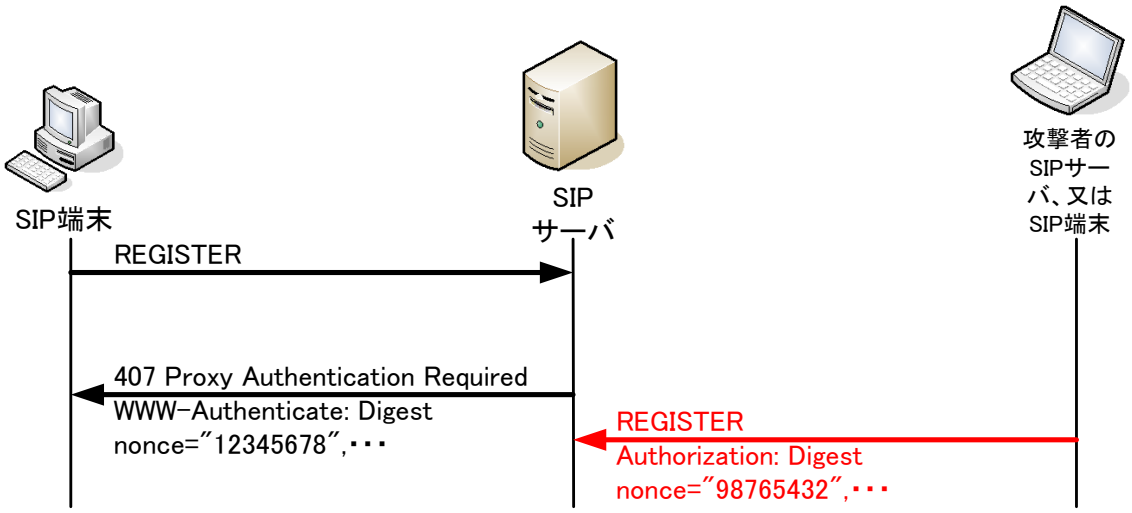


図 14-1 不適切な nonce チェックを悪用した偽装リクエストの送信

【原因と考察】

SIP のダイジェスト認証は、SIP リクエストを受けた SIP サーバや SIP 端末(UAS)が 407 か 401 のレスポンスに認証要求の情報を載せて SIP レスポンスを返すことで始まる。

この認証要求の中には、偽装リクエストに対する耐性を高めるために、nonce,opaque などのパラメータが含まれている。

```
WWW-Authenticate: Digest
realm="biloxi.com",
qop="auth,auth-int",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

【 項目 14. 認証機能の不十分な実装の問題 】

SIP リクエストに対して、401/407 レスポンスで認証要求を受けた SIP 端末(UAC)は認証情報を追加した SIP リクエストを再送する。

```
Authorization: Digest username="bob",
realm="biloxi.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
uri="sip:bob@biloxi.com",
qop=auth,
nc=00000001,
cnonce="0a4f113b",
response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

このとき、cnonce や nc などのデータを追加して、ハッシュ値(response)を計算する。

nonce,opaque は認証要求が生成される都度、サーバや UAS が新たに生成する値である。cnonce は認証要求に対して UAC が生成するランダムなトークンで、任意のタイミングで新しい cnonce に変更できる値である。cn は同じ cnonce を使い続ける場合のカウントで 1 から始まりで 1 ずつ増えていく値である。

認証情報をチェックする側は自分が生成した認証要求や最新の認証情報のパラメータを記憶し、チェックする必要がある。例えば、自分が生成していない nonce パラメータを許容してしまうと、偽装メッセージの生成時に本来は認証要求をキャプチャしなければならないパラメータを、ランダムに生成するだけでよくなり、偽装の難易度が下がってしまう。また、nc の増加をチェックしないようなサーバは、キャプチャしたリクエストのリプレイ攻撃を受け付けてしまうことになる。

14.3 対策

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【実装ガイド】

1) データのチェックを徹底する
   ダイジェスト認証を実装する際には、変化すべきでないデータと、変化していなければならないデータをしっかりチェックしなければならない。
   サーバ/UAS での認証情報に関するヘッダレベルのチェック項目は以下のようになる。

   ① Call-ID ヘッダが同じか
   ② From ヘッダが同じか(IP 電話で非通知の場合は除く)
   ③ CSeq が増えているか
   ④ SIP リクエストの種類(SIP メソッド)が同じか
   ⑤ To ヘッダが同じか

【 項目 14. 認証機能の不十分な実装の問題 】

また、サーバ/UAS での認証ヘッダのチェック項目は以下のようになる。

① username の登録チェック
② uri の登録チェック
③ realm が認証要求と同じか
④ nonce が認証要求と同じか
⑤ opaque が認証要求と同じか
⑥ nc は前回から増えているか(初回なら次回に備えて記憶)
⑦ cnonce が新しい(初回:nc=1)なら次回に備えて記憶、古い(2 回目以降)なら前回と同じか
⑧ response は正しいハッシュ値か

2) クライアントは cnonce を定期的に変更する
3) サーバからも認証要求のパラメータを定期的に更新(nonce,opaque)する
クライアントはサーバからのパラメータ変更に対応できるように実装する必要がある
4) Secure SIP (SIP over TLS)の実装

【 項目 14. 認証機能の不十分な実装の問題 】

14.4 参考情報

公開年月	情報源
1999 年 6 月	RFC2617 HTTP Authentication: Basic and Digest Access Authentication http://tools.ietf.org/html/rfc2617
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol 22 Usage of HTTP Authentication http://tools.ietf.org/html/rfc3261#section-22
2007 年 3 月	Sipera への報告 Insufficient integrity checks on SIP digest authentication messages http://www.sipera.com/index.php?action=resources,threat_advisory&tid=179&
2007 年 3 月	Sipera への報告 Absence of server authentication during SIP digest authentication http://www.sipera.com/index.php?action=resources,threat_advisory&tid=180&
2007 年 3 月	Sipera への報告 Registrar honors replayed authentication parameters http://www.sipera.com/index.php?action=resources,threat_advisory&tid=181&
2007 年 3 月	Sipera への報告 No cross-check performed between username of user requesting authentication and username used in credentials during SIP digest authentication http://www.sipera.com/index.php?action=resources,threat_advisory&tid=182&
2007 年 3 月	Sipera への報告 Some implementations of SIP Proxy may honor replayed authentication credentials http://www.sipera.com/index.php?action=resources,threat_advisory&tid=183&
2007 年 3 月	Sipera への報告 Service provider call feature servers may be vulnerable to service theft when sent a replayed and spoofed feature invocation message http://www.sipera.com/index.php?action=resources,threat_advisory&tid=188&
2007 年 3 月	Sipera への報告 Service provider call feature servers may be vulnerable to call hijacking http://www.sipera.com/index.php?action=resources,threat_advisory&tid=189&
2008 年 10 月	Analysis of a VoIP Attack (Klaus Darilion, IPCom) http://www.ipcom.at/fileadmin/public/2008-10-22_Analysis_of_a_VoIP_Attack.pdf 2008 年 10 月、ドイツの VoIP ユーザ向けの大量着信事件は、「インターネット上の IP 電話から一般電話網への無料の中継を可能にするプロキシを探すものだった」とする指摘。 SIP サーバ、SIP proxy、SIP ゲートウェイは、特定のレルムや、認証済みのユーザからの発信呼以外は中継しないよう、注意喚起している。

【 項目 14. 認証機能の不十分な実装の問題 】

14.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	□ Ⅰ（注意）	■ Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値		5.1	

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□ 隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	□なし	■部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

項目15. 送信元 IP アドレスを確認しない実装の問題

15.1 概要

SIP サーバのソース IP アドレスを確認しない端末実装では、他の第三者から SIP サーバになりすましたメッセージを受信してしまう可能性がある。

15.2 解説

【攻撃手法とその影響】

図 15-1 のように、攻撃者は任意の SIP リクエストを偽装して、攻撃目標の SIP 端末に送信する。

SIP 端末が、SIP サーバから受信したリクエストは無条件に信頼するという設定で動作しているにも拘らず、受信した INVITE リクエストの IP アドレスを SIP 端末が確認しないような実装であった場合、SIP 端末は不正な SIP リクエストを処理してしまう可能性がある。

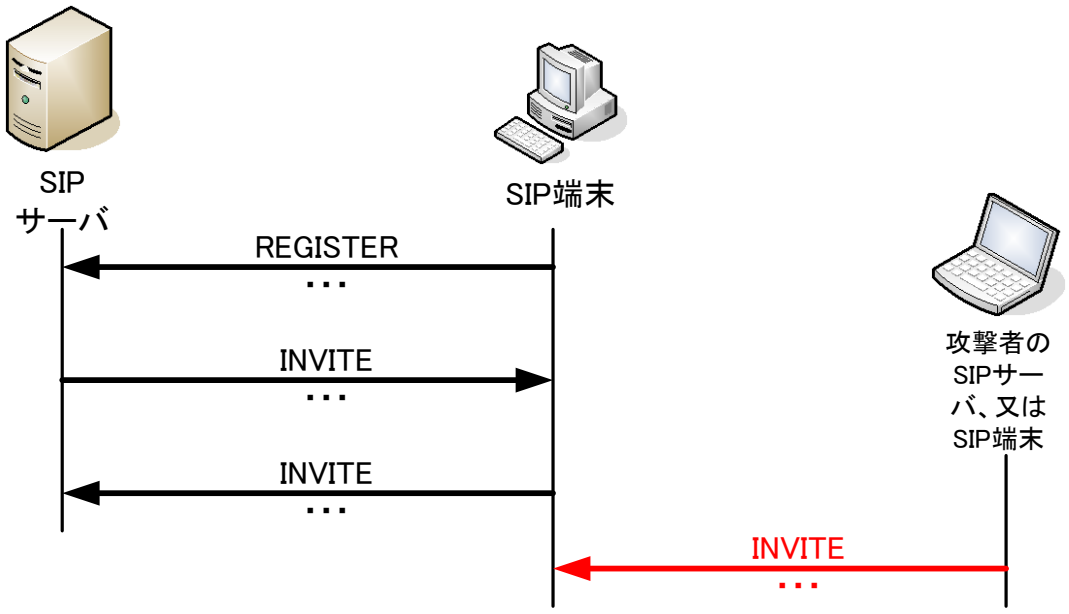


図 15-1 受信リクエストのソース IP アドレスを確認しない端末

【原因と考察】

SIP 端末は、リクエストの送受信を仲介するプロキシサーバが設定できるようになっていることが多く、REGISTER リクエストや INVITE リクエストの送信先として使われたり、SIP 端末への INVITE リクエストの送信元となる。SIP 端末はリクエストの送信時に SIP サーバから認証を要求されるのが一般的であるが、SIP サーバから SIP 端末へ送信される際に SIP 端末が認証要求を出すこと例は少ないと考えられる。この理由として、着信 SIP 端末が全ての発信 SIP 端末に関する認証情報を持つことが実用上困難であることが考えら

れる。システム全体は、発信側の SIP 端末の正当性は SIP サーバが確認し、SIP サーバは正しい SIP 端末にリクエストを送信するという前提で動作しているものと考えられる。

このことにより、受信リクエストの正当性はサーバがチェック済みだという前提で受信側 SIP 端末が動作可能となり、端末でのセキュリティに対する要件を少なくすることができる。しかし、限定された SIP サーバからのリクエストだという点に関する信頼性の上に成立する運用ポリシーであることから、この信頼性の確保が十分でない場合、端末でのセキュリティに重大な問題が発生する可能性がある。

15.3 対策

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【実装ガイド】

1) Secure SIP (SIP over TLS)の実装
2) IP ヘッダによるアドレスのチェック

15.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol http://tools.ietf.org/html/rfc3261
2006 年 6 月	TTC 標準 JJ-90.24「事業者 SIP 網に接続する SIP 端末基本接続インタフェース技術仕様」 http://www.ttc.or.jp/j/document_list/sum/sum_JJ-90.24v2.pdf (概要) 4.1.3.2 Contact ヘッダの扱い
2007 年 3 月	Sipera への報告 Endpoints vulnerable to accepting requests from source IP other than the specified server http://www.sipera.com/index.php?action=resources,threat_advisory&tid=186&

【 項目 15. 送信元 IP アドレスを確認しない実装の問題 】

15.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	□ Ⅰ（注意）	■ Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値		5.0	

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	□高	□中	■低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	■なし	□部分的	□全面的
完全性への影響	■なし	□部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

項目16. 不適切な IP アドレスを含む SIP メッセージに関する問題

16.1 概要

SIP メッセージ中には、複数箇所に IP アドレスが記述されているが、SIP の処理上問題のある IP アドレス(ループバックアドレス、自端末のアドレスやブロードキャストアドレスなど)をチェックしない実装では、サービス不能状態になったり、再起動しなければならないような状態になってしまう可能性がある。

16.2 解説

【攻撃手法とその影響】

偽装された INVITE リクエストの SDP にループバックアドレス(127.0.0.1)を記述したり、Via ヘッダや Contact ヘッダにブロードキャストアドレスや受信端末の IP アドレスを記述して攻撃対象の端末に送信する。このことにより、メディアを自分自身と送受信したり、レスポンスを自分自身に送信するという結果になる。自己ループ状態になった端末はサービス不能な状態になったり、再起動が必要な状態になる可能性がある。

図 16-1 は攻撃者の SIP 端末、あるいは SIP サーバが INVITE リクエストの Via ヘッダや SDP の c 行に、不適切な IP アドレスを記述している例ある。

Via ヘッダに受信 SIP 端末の IP アドレスを記述した場合、受信端末は SIP レスポンスを受信 SIP 端末、つまり自分自身に送信してしまうことになる。また、SDP の c 行にループバックアドレスが記述されていると、受信 SIP 端末は音声やビデオなどのメディアをやはり自分自身に送信してしまう可能性がある。

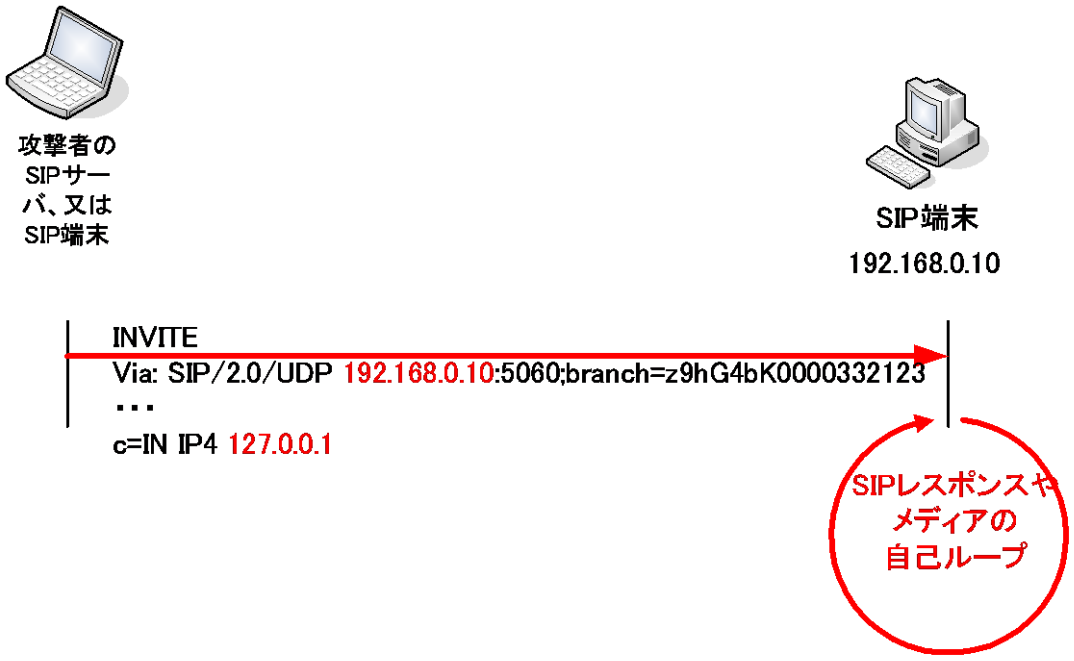


図 16-1 SIP レスポンスやメディアの自己ループを引き起こす SIP リクエスト

【 項目 16. 不適切な IP アドレスを含む SIP メッセージに関する問題 】

【原因と考察】

SIP メッセージは、以下の箇所などに IP アドレスとポート番号が記述される。

1) Request URI
2) Via ヘッダ
3) Contact ヘッダ
4) Route ヘッダ
5) Record-Route ヘッダ
6) SDP 内の c 行

1), 3), 4)はリクエストの送信に関係するアドレス情報なので、SIP サーバと SIP 端末の両方に対して影響がある。

2)はレスポンスの送信に関係するアドレス情報なので、やはり SIP サーバと SIP 端末の両方に対して影響がある。

5)は直接リクエストやレスポンスの送信に関係するわけではないが、新たなリクエストの送信時に Route ヘッダの情報として扱われるため、最終的には SIP サーバと SIP 端末の両方に対して影響がある。

6)は SIP 端末あるいは、SIP 端末として動作するメディアゲートウェイが、音声やビデオなどのメディアを送信する際に使用されるので、広義には SIP 端末、狭義には SIP 端末のメディアゲートウェイに影響があると考えられる。

これらは、シグナリングやメディアの送受信に必要な情報であるが、ループバックアドレスや、ブロードキャストアドレスなど明らかに不適切なアドレスでもプロトコル上は記述できる。これらのアドレス情報はアプリケーションレイヤでチェックすべきだが、無条件に使用される実装が存在する。

16.3 対策

【運用ガイド】

1) IPsec、SSL-VPN などの暗号化トンネルを使って SIP 通信を保護する
2) SIP/RTP ネットワークを隔離する、閉じたネットワークを利用する
3) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する
4) SIP サーバによるチェック
   途中の SIP サーバでヘッダやボディ内に記述されている IP アドレスやポートの正当性を検証し、不適当と判断された場合はエラーを返したり、リクエストを破棄する

【実装ガイド】

1) Secure SIP (SIP over TLS)の実装
2) IP アドレスのチェック

【 項目 16. 不適切な IP アドレスを含む SIP メッセージに関する問題 】

ループバックアドレス、自端末の IP アドレス、ブロードキャストアドレスなど不適切な IP アドレスが記述されていないかをチェックする

3) UDP/TCP のポート番号のチェック
ポート番号についても、0 から 1023 までの well known ポートと呼ばれるポートが記述されていないか、また、SDP の m 行に SIP と同一のポートが記述されていないかチェックする

16.4 参考情報

公開年月	情報源
2002 年 6 月	RFC3261 SIP: Session Initiation Protocol http://tools.ietf.org/html/rfc3261
2007 年 3 月	Sipera への報告 Implementation flaws may allow remote attacker to exploit improperly handled error conditions http://www.sipera.com/index.php?action=resources,threat_advisory&tid=185&

16.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	□ I （注意）	■ II （警告）	□III （危険）
本脆弱性の CVSS 基本値		5.0	

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	□高	□中	■低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響	■なし	□部分的	□全面的
完全性への影響	■なし	□部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

【 項目 17. デバッガ機能へ接続可能な実装の問題 】

項目17. デバッガ機能へ接続可能な実装の問題

17.1 概要

卓上電話機タイプの SIP 端末や、電話機を接続して使用する IP 電話アダプタなどを作成する際には、組み込み OS と呼ばれる OS を使用することが多い。組み込み OS は、応答のリアルタイム性が高く、少ないメモリで動作するなどの要件があり、以下のような OS が代表的なものと考えられる。

1) ITRON
2) VxWorks
3) Linux
4) WindowsCE(Windows Mobile)

また、これらの OS 上で SIP 端末を開発する際には、Windows や Linux などの別プラットフォーム上で、バイナリコードをクロスコンパイルし、実際のハードウェアにアップロードして動作させるという開発手法が一般的で、この際ソフトウェアの起動状態、内部遷移状態、各種パラメータ等を実際に動作している状態で確認する手段として、リモートデバッグという手法が用いられる。リモートデバッグとは、組み込み OS が動いているハードウェア(ローカル側と呼ぶ)と、デバッグソフトウェアが動作している Windows や Linux などの開発マシン(リモート側と呼ぶ)をシリアルケーブルや、IP ネットワークで接続し、必要なデータをリモート側で読み出したり、ローカル側のデータを書き換えて実行させる処理である。このようなリモートデバッグ機能**に接続できてしまう製品がある**。

17.2 解説

【攻撃手法とその影響】

GDB(GNU Source-Level Debugger)などのリモートデバッガを使って、下記の手順で機器の OS (VxWorks など) 上で任意のバイナリコードを実行される可能性がある。

1) リモートホスト上のデバッガから、機器のデバッグポートへの接続
2) リモートホストから、機器内に任意のオブジェクトをダウンロードする
3) リモートホストから、機器内のオブジェクトを実行する

【 項目 17. デバッガ機能へ接続可能な実装の問題 】

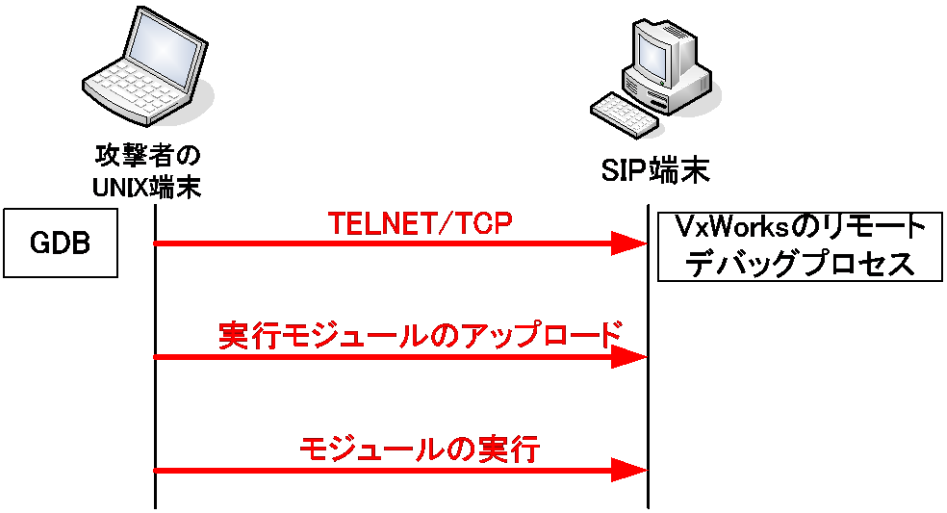


図 17-1 リモートデバッガによる不正なモジュールの実行

【原因と考察】

リモートデバッグ機能は、開発時に非常に有効な機能であるが、製品出荷時には停止させなければならない。本節の問題は、この機能をオフにしないで製品を出荷していることである。ポートスキャンを行えば容易に接続ポートは判明してしまい、特定環境での初期設定を知っていれば接続できてしまう可能性がある。リモートデバッグ機能は強力なバックドアとして働くため、開発環境以外でこの機能を使うことは非常に危険である。

17.3 対策

【運用ガイド】

1) ファイアウォールや侵入検知システムなど、製品とネットワークとの間で、この脆弱性を狙ったパケットを遮断、制限する装置を挿入する

【実装ガイド】

1) デバッグ機能の停止
製品を出荷する際には、デバッグ機能を使えないように設定する

【 項目 17. デバッガ機能へ接続可能な実装の問題 】

17.4 参考情報

公開年月	情報源
2006 年 9 月	Hacking VoIP Phones:802.11b/g Wireless & Wired http://www.io.com/~shawnmer/voipsecexp/noconname_2006_Merdinger.pdf
2006 年 7 月	Hacking VoIP Exposed http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Endler.pdf
2005 年 11 月	Cisco 7920 Wireless IP Phone VxWorks Remote Debugger Access Vulnerability http://www.securityfocus.com/bid/15456
2007 年 10 月	Debugging with GDB 18.2.1 Using GDB with VxWorks http://sourceware.org/gdb/current/onlinedocs/gdb_19.html#SEC182

17.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	□ I （注意）	■ II （警告）	□III （危険）
本脆弱性の CVSS 基本値		6.0	

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	□高	■中	□低
攻撃前の認証要否	□複数	■単一	□不要
機密性への影響	□なし	■部分的	□全面的
完全性への影響	□なし	■部分的	□全面的
可用性への影響	□なし	■部分的	□全面的

【 項目 18. 管理機能に関する問題 】

項目18. 管理機能に関する問題

18.1 概要

SIP 関連プロトコルを利用した機器で、SIP 関連プロトコル以外の、管理、設定、監視などの機能や使い方に脆弱性が含まれていることがある。これら脆弱性を利用して、攻撃者は管理権限を奪取したり、ID やパスワード、構成情報を収集できる。

18.2 解説

SIP 関連プロトコルを利用する機器は、TCP/IP をベースにした複数の機能から構成されていることが一般的である。ここでは SIP 関連プロトコル以外の、管理機能と管理設定に関する問題について説明する。

ここで言う管理機能とは、SIP 関連プロトコルを利用する機器を適切安全に利用するために、必要な設定を行ったり、機器を構成したりするための機能を指す。こうした管理機能が適切に利用されていなかったり、機器の出荷時の設定が不適切な場合に問題が発生することがある。

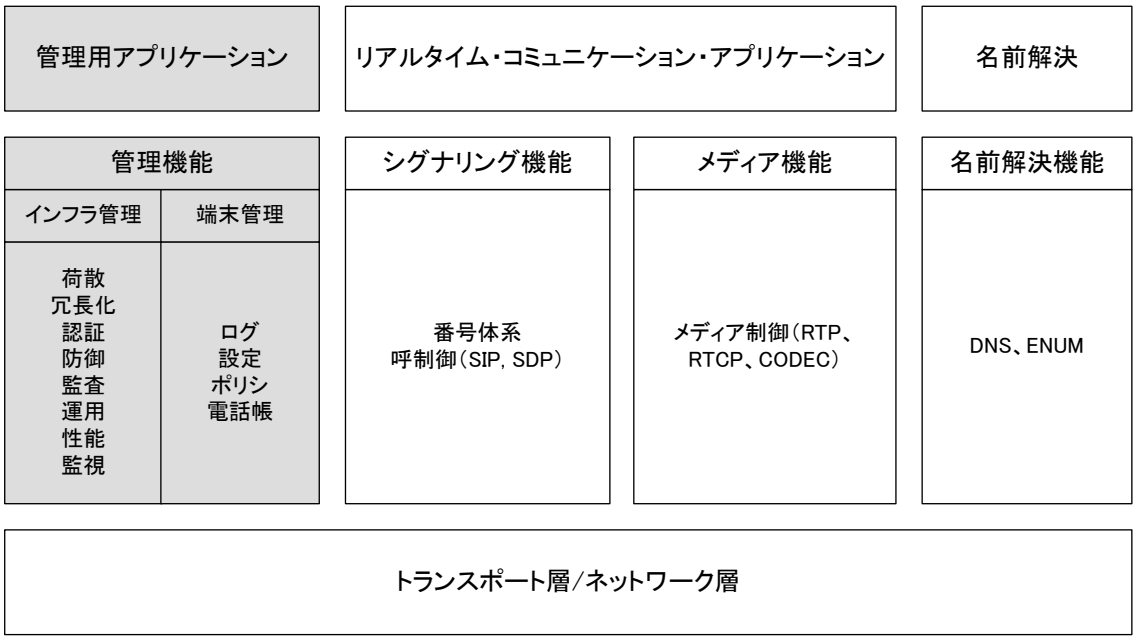


図 18-1. 管理機能などの SIP 関連以外の攻撃対象

【 項目 18. 管理機能に関する問題 】

【攻撃手法とその影響】

1) 管理 I/F のアクセス認証の問題

SIP 関連プロトコルを利用する製品､機器の設定管理インターフェースにはいくつかの方法がある。代表的な方法には以下のような方法がある。

① Web ページによる設定管理ページ(HTTP サーバ)
② コマンドラインによる設定管理コンソール（TELNET､RLOGIN､SSH など）
③ その他のネットワーク管理プロトコルによる設定（SNMP WRITE など）

これらの方法で設定管理機能が提供されるときに、認証なしに設定変更ができるようになっていたり、マニュアルに記載されたデフォルトの ID とパスワードがそのまま使えるようになっていて、他のネットワークの任意のホストに対して応答するものがある。

攻撃者は設定管理機能を利用して、その SIP 関連機器が利用する SIP プロキシサーバの IP アドレスを変更して、その機器が利用する SIP セッションをすべて盗聴したり、その機器の SIP セッションのすべてに介入することができるようになる。その結果、本資料で紹介した SIP/RTP への攻撃が非常に実行しやすくなる。

2) 設定･構成情報をダウンロードするプロトコルが保護されていない問題

SIP 関連プロトコルを利用する製品､機器の設定情報や構成情報をダウンロードするために使われる、TFTP をパケットキャプチャすることで、攻撃者は設定に含まれる ID とパスワード、その他の構成情報を収集できる。また、一部の機器では、任意のリモートホストに対して､機器の MAC アドレスとファームウェアのバージョン番号を無制限に応答するものもあった。

攻撃者に設定管理用の ID とパスワードが漏れれば、攻撃者はその機器を自由に設定変更できるようになる。すると、攻撃者は偽装した SIP プロキシサーバを設定して、その機器が利用するすべての SIP セッションを盗聴したり、SIP セッションに介入できるようになる。

3) ファームウェア更新ができない､または更新が遅い問題

SIP 関連プロトコルを利用する製品､機器の一部には、ファームウェアの更新機能がないものや、非常にしにくいものがある。また、メーカによっては機器の脆弱性が発表されても、ファームウェアの更新が半年以上にわたって提供されない場合がある。

既知の脆弱性を持ちながら、脆弱性対策がしにくい機器を狙って、攻撃者は容易に機器への攻撃を行うことができる。

4) 製品のドキュメント不足から起こる問題

SIP 関連プロトコルを利用する製品のマニュアル(取り扱い説明書)などのドキュメント、が不足していることがある。特に、運用上の脆弱性につながる重要事項が説明されていない場合に問題がある。

例えば、機器が持つ専用の管理プロトコルの存在と、製品出荷時の動作状況がドキュメントに書かれていないと、導入設計時にファイアウォールで適切に保護されず、容易な攻撃を許してしまうことがある。また、出荷時の管理用の ID とパスワードの内容と、ネット

【 項目 18. 管理機能に関する問題 】

ワーク経由での利用条件についても、利用者に説明されていないと、ID とパスワードが適切に管理・防御されない。

【原因と考察】

管理機能に関する問題は、脆弱性を研究する分野では「設定の問題」とも言われている。しかし、本資料ではあえて管理機能の問題とした。その理由は、設定作業は管理機能がなければ行うことはできず、管理機能が適切な設定方法やデフォルト値を提供することが非常に重要だからである。

1) 管理 I/F のアクセス制限方法の問題

機器や製品の設定変更やパスワード変更などを行う、管理インターフェース(I/F)を利用することは、機器を乗っ取ろうとする攻撃者にとっても、たいへん利用価値が高い手段である。管理 I/F のアクセス制御は、攻撃者や許可されない第三者の利用を制限するための重要な機能である。

一般的には、SIP 関連プロトコルを利用する機器は出荷時に管理者パスワードを設定したり、機器の起動時に TFTP などによって設定ファイルをダウンロードすることでアクセス制限方法が設定される。

出荷時に管理者パスワードを設定する方法は、取扱説明書などにパスワード文字列を書いて利用者に渡すことになり、誰にでも知られやすいものとなる。そのため、機器や製品の起動時に、パスワードを更新するまではネットワークに接続しないか、機器と同じ IP セグメントに対してだけ管理 I/F へのアクセスを許可する、などのアクセス制限が必要とされる。

2) 設定・構成情報をダウンロードするプロトコルが保護されていない問題

もともと TFTP はルータやスイッチなどのネットワーク機器の設定情報をファイルの形でサーバに置いて集中管理するために利用されているプロトコルである。TFTP は特に組み込み機器用に、認証なしの簡単な手順でファイルをダウンロードできるプロトコルで、UDP 上で利用する。通常、TFTP に暗号化機能はなく、ファイルの内容をそのまま UDP パケットで転送する。

本来 TFTP は管理用に利用するため、通信事業者などの運用者は管理専用のネットワークを物理的または論理的に分離して、一般ユーザや第三者が TFTP サーバにアクセスできないようにするのが普通である。具体的には、ネットワーク機器の管理用 Ethernet ポートや管理用 IP アドレスを、VLAN やトンネルを使って分離する。

IP 電話機などの SIP 関連機器では、簡易な実装と処理が可能なため、TFTP を利用した構成情報のダウンロードやファームウェアの更新ができるようにしている。しかし、IP 電話機のような機器にも、ルータやスイッチ並みの管理通信の保護が適用されていないと、構成情報が第三者に漏れてしまうことになる。

3) 管理用 WEB ページ上に XSS 脆弱性、XSRF 脆弱性、SQL インジェクション脆弱性がある問題

管理用 WEB ページに、XSS(クロスサイトスクリプティング)脆弱性や XSRF(クロスサイトリクエストフォージュリ)脆弱性があると、管理者のブラウザを経由して、管理 WEB インターフェースに任意の JavaScript を埋め込まれて実行されたり、利用者が意図しない操作を勝手に行われることがある。その結果、管理 WEB インターフェースが攻撃者によって事実上、乗っ取られてしまうことがある。また、管理 WEB サーバ内に SQL インジェクション脆弱性があると、やはり管理 WEB が提供していない機能まで含めてデータベース機能

の制御が奪われる。
管理 WEB ページ上の XSS 脆弱性、SQL インジェクション脆弱性の問題は、SIP サーバ機能が複雑になるのに従って、IP-PBX などにおいても事例が報告されるようになった。また、管理機能の乗っ取りにより、IP 電話サービスの不正な利用や課金情報の不正操作への危険性も指摘されている。

4) ファームウェア更新ができない、または更新が遅い問題

ファームウェアの更新機能は Web ブラウザで利用できる機器が多いが、一部の機器は保守用のシリアルポートや、フラッシュメモリカードの交換などで更新機能が提供されていたり、機器そのものをメーカに返送して書き換えてもらう場合もある。
シリアルポートは直接 IP ネットワークに接続できないため、ファームウェアを更新するためには機器が設置してある現場に出向くか、機器を管理者の手元に移動しなければならない。フラッシュメモリカードを交換する場合も、同様である。
メーカへの機器の返送には輸送期間と費用がかかることや、その間機器が利用できなくなることから、ファームウェアの更新は非常にしにくいものとなる。
ファームウェアの更新が遅いメーカの問題は、格安の機器を販売しているメーカや、保守サービスを提供していないメーカに目立つ。どうしても格安の機器を利用する場合は、脆弱性対策として運用上の対応策をとる必要がある。

18.3 対策

【運用ガイド】

1) 導入機器の初期設定をどのようにするか、機器の安全対策説明書や取扱説明書の注意事項を理解してから、検討・設置を行う。
2) 導入機器は設置前にポートスキャンをしておくと、ドキュメント化されていないネットワークポートがわかることがある。
3) 脆弱性が発見されたあとの対策方法をメーカといっしょに検討しておくこと。
4) HTTP は SSL/TLS 上で利用する。

【実装ガイド】

1) 出荷時パスワードと管理者アクセスの制限など、出荷時直後の製品、機器に容易に管理者アクセスができないようにする必要がある。
2) 製品が提供する機能はもらさずドキュメント化する必要がある。
3) 脆弱性が発見されたあとの対策方法を検討しておく
4) HTTP などの関連プロトコルを使った機能の脆弱性にも十分な配慮が必要である。
管理 WEB ページについては「安全なウェブサイトの作り方」をチェックする。

【 項目 18. 管理機能に関する問題 】

18.4 参考情報

公開年月	情報源
2005 年 5 月	Vulnerabilities in SOHO VoIP Gateways Peter Thermos and Guy Hadsall, The VoPSecurity.org Forum http://www.vopsecurity.org/papers/Security_Issues_with_SOHO_VoIP_Gateways-052005.pdf 管理 I/F、デフォルトパスワードの問題を含む家庭用機器の問題を広く指摘する資料
2005 年 10 月	VOIPSA - VoIP Security and Privacy Threat Taxonomy http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf VoIP セキュリティ全般の脅威を網羅的に分類した例。OS や TCP/IP も含む。
2006 年 12 月	Hacking VoIP Exposed - David Endler and Mark Collier for BlackHat 2006 http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Endler.pdf SNMP、TFTP が保護されていない問題を含む VoIP セキュリティへの警告。
1999 年 6 月	RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1 http://tools.ietf.org/html/rfc2616 HTTP プロトコルの RFC
2000 年 5 月	RFC2818 - HTTP Over TLS http://www.ipa.go.jp/security/rfc/RFC2818JA.html [日本語] TLS 上での HTTP の利用方法を定義する RFC。
1983 年 5 月	RFC854 - TELNET PROTOCOL SPECIFICATION http://tools.ietf.org/html/rfc0854 TELNET のプロトコルを定義する RFC
2003 年 4 月	RFC3512 - Configuring Networks and Devices with Simple Network Management Protocol (SNMP) http://tools.ietf.org/html/rfc3512 SNMP でネットワーク機器の設定を行うときの注意点をまとめた RFC。
2003 年 8 月	RFC3584 - Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework http://tools.ietf.org/html/rfc3584 SNMP を利用する際は認証機能、暗号化機能があるバージョンとないバージョンの複数の SNMP を実装することを勧める RFC。
1991 年 12 月	RFC1282 – BSD Rlogin http://tools.ietf.org/html/rfc1282 RLOGIN プロトコルの RFC
2007 年 3 月	IPA – Secure Shell http://www.ipa.go.jp/security/rfc/RFC.html#13 SSH 関連の RFC 一覧

【 項目 18. 管理機能に関する問題 】

公開年月	情報源
1992 年 7 月	RFC1350 - THE TFTP PROTOCOL (REVISION 2) http://tools.ietf.org/html/rfc1350 TFTP プロトコルの RFC
2007 年 12 月	Cisco Unified IP Phone Remote Eavesdropping http://www.cisco.com/en/US/products/products_security_response09186a0080903a6d.html Ciscon の統合型 IP 電話で、外線移動設定を悪用し、遠隔から盗聴できる問題。 Remote Wiretapping on Cisco Phones http://www.hack.lu/archive/2007/hacklu07_Remote_wiretapping.pdf Cisco IP 電話 7940 の外線移動設定のための情報は、IP 電話機の管理ページの非暗号通信から傍受できるという手順を示す例。
2007 年 10 月	Owning the internal network with SIP (part 1) and a Linksys Phone http://seclists.org/fulldisclosure/2007/Oct/0174.html LynkSys SPA-941 で XSS(クロスサイトスクリプティング)を利用して管理機能を乗っ取られる問題。
2007 年 10 月	[VOIPSEC] XSS and SQL injection via SIP (part 2) and toll fraud bonus http://voipsa.org/pipermail/voipsec_voipsa.org/2007-October/002466.html XSS を利用して IP-PBX の管理機能が乗っ取られ、SQL インジェクションによって通信の課金記録が消去される問題の指摘。Asterisk の追加機能に共通の問題。(Areski, FreePBX, Tribox)
2008 年 4 月	Australians falling victim to foreign phone hackers http://www.livenews.com.au/Articles/2008/04/17/Australians_falling_victim_to_foreign_phone_hackers オーストラリア、メルボルンの企業と大学 2 組織で、IP 電話システムが悪用され、合計 10 万ドルの海外通話料金が請求されたというニュース。原因、手口は未確認。
2008 年 6 月	IPA「安全なウェブサイトの作り方 改訂第 3 版」 http://www.ipa.go.jp/security/vuln/websecurity.html SQL インジェクション、XSS、アクセス制御や認可制御の欠落など、 ウェブサイトに関する脆弱性の届出件数の約 9 割を網羅する対策資料。

【 項目 19. 登録 ID と構成情報の収集に関する問題 】

項目19. 登録 ID と構成情報の収集に関する問題

19.1 概要

SIP 関連プロトコルを利用する製品、機器に対して複数の方法で、登録された ID や、内部の構成情報を収集される場合がある。

1) インターネット検索エンジンを利用して機器の管理ページなどを検索される問題
2) ネットワーク管理プロトコルである SNMP の問い合わせに応答してしまう
3) SIP アドレスが番号であるときの問題: 連続した数字による番号を予測される
4) SIP の盗聴と応答方法の問題: SIP の通信をパケットキャプチャされて ID の一覧を収集される
5) SIP サーバに応答を促すメッセージを送られて、ID の一覧を収集される

19.2 解説

【攻撃手法とその影響】

1) インターネット検索エンジンを利用して機器の管理ページなどを検索される問題

インターネット検索エンジンを利用して、SIP 関連プロトコルを利用する製品、機器が内蔵している管理ページに特有のキーワードや検索キーを指定して検索する。検索結果として、インターネットからアクセス可能な、稼動中の製品や機器の管理ページ、稼働中の製品の IP アドレスの一覧を収集できる。

攻撃者は稼働中の製品の管理ページにインターネット経由でアクセスし、製品の出荷時の管理用 ID とパスワードを試して、SIP プロキシサーバや SIP アドレス、DNS や NTP のアドレスなどの管理情報を収集することができる。一般的に、基本的な SIP/RTP 製品の管理ページに含まれる設定情報には次のようなものがある。

① SIP サーバ: ホスト名または IP アドレス
② SIP プロキシサーバ: ホスト名または IP アドレス
③ RTP プロキシサーバ: ホスト名または IP アドレス
④ SIP URI アドレス(ユーザ名、レルム名)
⑤ SIP 登録(REGISTER)用のユーザ名とパスワード
⑥ SIP/RTP の待ちうけ UDP ポート番号
⑦ NTP サーバ: ホスト名または IP アドレ
⑧ TFTP サーバ: ホスト名または IP アドレス
⑨ STUN サーバ: ホスト名または IP アドレス
⑩ SNMP コミュニティ名、SNMP 認証鍵
⑪ DHCP の指定
または固定 IP アドレス、デフォルトルータ IP アドレス、DNS サーバ IP アドレス

また、検索エンジンを利用した情報収集では、特定組織の電話番号を収集して、複数の部署や関連会社をまたがった、電話番号と窓口の一覧が取得できる。さらに、場合によっては公開されるべきではない、組織内の電話番号や、内線番号も収集できる場合がある。

【 項目 19. 登録 ID と構成情報の収集に関する問題 】

2) SIP アドレスが番号であるときの問題: 連続した数字による番号を予測される問題

SIP アドレスが既存の公衆電話網に使われているような、連続した数字である場合、攻撃者はコンピュータプログラムやバッチ処理を使って連続した番号に発信することで、大量の SIP アドレスに対して自動的に電話発信ができる。

スパム(SPAM)と呼ばれる、迷惑メールと同じ手口と同じように、IP 電話を使った迷惑電話を、SPIT(Spam for Internet Telephony)などと呼ぶ。SPIT では、攻撃者は IP 電話の受信者に対して、自動的に商品を説明する音声データを再生したり、偽の「ID やパスワードの入力」といった詐欺を実行する。偽のガイダンスに従って、テンキーを押して ID やパスワードを入力すると、攻撃者はトーン信号の音声認識処理によって、ID とパスワードが攻撃者の手に渡ってしまう。

3) ネットワーク管理プロトコルである SNMP の問い合わせに応答してしまう問題

SIP 関連プロトコルを利用する製品、機器が SNMP(Simple Network Monitoring Protocol: ネットワーク管理プロトコル)に応答することがある。攻撃者は機器の一覧や構成情報を得るために、SNMP のデフォルトポート番号で特定の IP アドレスを持つホストに、よくある SNMP コミュニティ名を指定して問い合わせを行うと、機器が SNMP の問い合わせに応答してしまうことがある(SNMP Read)。

応答する機器に対しては、SNMP Walk と呼ばれる、構成情報を繰り返し再帰的に問い合わせる処理を行い、ネットワークインターフェースの一覧や、IP アドレスの一覧、オープンしているポートの一覧やホスト名などの構成情報をとりだされてしまう。

また、SNMP を使った、機器への設定投入も可能な場合(SNMP Write)、攻撃者が機器の設定を勝手に変更してしまうこともある。

4) SIP の通信をキャプチャされて ID の一覧を収集される問題

保護されていない SIP の通信をパケットキャプチャして、SIP のヘッダにある SIP URI を収集することで、SIP 通信に使われている SIP の ID 一覧を攻撃者に収集される。

攻撃者は ID の一覧を利用して、別の攻撃を行う準備をする。

5) SIP サーバに応答を促すメッセージを送られて、ID の一覧を収集される問題

SIP サーバの実装の中には、SIP の OPTIONS 要求や SIP の REGISTER 要求に対して、SIP アドレスが存在するかどうかわかるような応答を返すものがある。こうした応答を判別することで、ありがちな SIP アドレスの一覧を SIP サーバに問い合わせ、実際に SIP サーバに登録されている SIP アドレスの一覧を選別することができる。

攻撃者は SIP アドレスの一覧を利用して、別の攻撃の準備を行う。

【原因と考察】

1) インターネット検索エンジンを利用して機器の管理ページなどを検索される問題

一般に、インターネット検索エンジンを利用した、非公開情報の収集手法は、「検索エンジンハッキング」などと呼ばれる。最初にまとめられた検索例は 2003 年の Defcon 11 の資料「Watching the Watcher」に見られる。

もともとインターネット検索エンジンは、「クローラー」または「ボット」などと呼ばれるソフトウェアを使って、自動的にインターネットから Web ページを収集している。クロ

【 項目 19. 登録 ID と構成情報の収集に関する問題 】

ーラーは一般公開されている Web のみを収集しており、一般的にインターネット検索エンジンのクローラーは、ID やパスワードを使わずに閲覧できるページだけを収集している。

しかし、IP 電話機や呼制御サーバなどの SIP 関連プロトコルを利用する機器を、インターネットに公開されたページからリンクしてしまったり、機器へのアクセス履歴や、ログファイルの一覧などを一般に掲示公開すると、インターネット検索エンジンのクローラーにも Web ページが収集されてしまう。

一旦、Web ページが収集されると、インターネット検索エンジン上で特定のキーワードを指定すれば検索可能となる。一部のインターネット検索エンジンにある検索オプションで、「タイトル内文字列検索 ”intitle:”」や「URL 内の文字列検索 ”inurl:”」などを利用すると、簡単に管理ページや特定の設定ページを検索できる。また、「数字..数字」という検索パターンでは、連続した数字の範囲を検索することができるため、電話番号の検索に利用できる。

インターネット検索エンジンでは、一般公開された情報を収集し、それを検索できるようにしているが、検索文字列から、必ずしも悪意があるかどうかを特定することはむずかしい。そのため、基本的にはサイト管理者が秘密にしておくべき情報は公開しないか、アクセス制限を適用するなどの、適切な対応が必要である。また、本報告書のほかの項目で指摘するように、SIP 関連機器は基本的に閉じたネットワークで利用することが望ましい。そのため、インターネットから SIP 関連機器をアクセス可能にするかどうかは、十分な配慮が必要である。

サイト管理者はクローラーを拒否することもできるよう、robots.txt というファイルに、Web ページの収集可否を宣言することもできるが、インターネット検索エンジンは必ずしも robots.txt に従っているとは考えられないため、robots.txt によるアクセス制限には限界がある。

検索エンジンハッキングが指摘する運用上の注意点としては、このほか、ディレクトリの一覧表示を行わないことや、開発途中のサイトやネットワーク情報のまちがった公開への注意、運用中のサイトの秘密情報を検索してみる確認作業、などを勧めている。悪意のある検索キーワードを収集してデータベース化しているサイトもあるので、Web サイト管理者やネットワーク管理者は定期的な検査をすることが求められる。

2) ネットワーク管理プロトコルである SNMP の問い合わせに応答してしまう

SNMP は組み込み型のネットワーク機器が標準的に搭載する、ネットワーク管理機能である。SNMP を使った管理サーバなどから、管理対象の機器に対して、SNMP の情報取得リクエストや情報設定リクエストを送信して、機器が構成情報を応答したり、機器内部の設定を変更する。

似たような機能は、HTTP 上での Web ページでの管理設定機能にもあるが、Web ページ上の管理設定機能は人間に対する GUI 提供が目的であるのに対して、SNMP はユーザインターフェースなしの管理機能のみの提供が目的にある。現在の設定管理の主流は GUI ベースの Web ページによる管理であり、一部の高機能機器では、XML をベースにした高度な設定や認証機能が提供されている。一方、SNMP は UDP 上で、簡単な認証機能と、単一のツリー状の名前付けルールによって統一的に設定や管理情報を参照できる。もともとルータやスイッチなどの組込機器が、あまりメモリや CPU を持っていなかった時代に考案されたプロトコルだが、IP 電話機やネットワーク対応プリンタのような簡易な組込機器にも搭載されている例が多い。

しかし、SNMP を実装した IP 電話機製品の多くが、出荷時の認証機能は無効になっており、識別名としての「コミュニティ名」も共通のものとなっている。また、機器出荷時の SNMP でのアクセス制限がなく、どのネットワークからも受け付けるようになっている。そのため、攻撃者から共通のコミュニティ名を使って問い合わせされると、応答してしま

うことが多い。
また、SNMP でアクセスできる構成情報(オブジェクト)は単一のツリー状になっているため、再帰的に所定のオブジェクト名を指定することで、ほとんどすべての構成情報にアクセスすることができる。
SIP 関連プロトコルを利用する機器を導入する場合は、SNMP へのアクセス方法を適切に制限する必要がある。また、導入後も定期的な検査が必要である。

3) SIP アドレスが番号であるときの問題: 連続した数字による番号を予測される

すでに公衆電話網でも問題になっているが、コンピュータによって自動化された発呼処理によって、セールスや詐欺を試みる攻撃者が存在する。このような手口を「SPIT」と呼ぶ。
連続した数字を使った電話番号体系を使う限り、連続した番号への自動発呼そのものを制限することはむずかしいが、受信する側での SPIT への対応方法が、IETF で議論されているので、参照してほしい。(A Framework for Reducing Spam for Internet Telephony)

4) SIP の通信をパケットキャプチャされて ID の一覧を収集される

SIP の通信を保護していない場合、SIP のヘッダには自ホストまたはあて先ホストの SIP アドレスが生のテキストで書かれているため、パケットキャプチャすれば SIP アドレスを収集することができる。
その他の SIP の脆弱性への対策と同様に、閉じたネットワークを利用するか、SIP の通信自体を TLS や IPsec などのプロトコルを利用して保護する必要がある。

5) SIP サーバに応答を促すメッセージを送られて、ID の一覧を収集される問題

SIP のパケットをキャプチャする方法が受身的な方法なのに対して、SIP サーバに対して問い合わせメッセージを送信して ID の一覧を得るため、この方法は能動的な方法である。
SIP サーバは、それぞれのリクエストに対して、相応のレスポンスを返す。このとき、レスポンスの内容を確認すると、ID が存在する場合と存在しない場合に、レスポンスが異なっている実装がある。
例えば、ID が存在しない場合の REGISTER リクエストに対して「その ID は存在しない」などと応答し、ID が存在する場合の REGISTER リクエストに対しては「認証が必要です」などと応答する場合である。このような応答をする SIP サーバに対して、よくある ID や辞書を使って、手持ちのすべての ID の問い合わせを行うと、SIP サーバ上にも存在する ID が確認できることになる。
一般に、SIP サーバは ID が存在するかどうかに関わらず、異なる応答をしないような実装が求められる。
なお、OPTIONS リクエストを利用して、SIP サーバや SIP プロキシサーバの存在を確認する手法もある。ID の収集対策も含めた対応をするためには、閉じたネットワークを利用するか、SIP の認証か別の認証結果を元にした SIP リクエストの利用制限を行う必要がある。

19.3 対策

【運用ガイド】

1) 閉じたネットワークを利用する
ルータやスイッチ上で Ethernet VLAN を利用したり、ファイアウォールなどで接続が制限され

【 項目 19. 登録 ID と構成情報の収集に関する問題 】

た、閉じたネットワーク内で SIP 関連機器を利用することで、インターネットからのアクセスや、無線 LAN 環境などで認証なしで接続しようとする端末のアクセスを遮断する。

2) IPsec などの暗号化トンネルプロトコルで SIP 通信を保護する
IPsec などの暗号化トンネルプロトコルを利用して SIP のヘッダが盗聴されないよう、SIP の通信を保護する。

3) 対策済みの SIP プロキシサーバを経由する
脆弱性を持つ SIP サーバをすぐに改修できない場合は、SIP 端末に対して、脆弱性に対応した SIP プロキシサーバを挿入し、SIP 通信が必ず経由するように構成する。同様に、SIP 対応の IDS(侵入検知システム)やファイアウォールを挿入することも候補として検討に値する。

【実装ガイド】

1) アクセス制御機能の提供
製品の管理設定ページまたは、SNMP などの管理設定機能へのアクセスを制限する機能を提供する。管理者権限を認証する機能、管理者接続を受け付ける範囲を IP アドレスの範囲や同一セグメントに限るなどして制限する機能が考えられる。

2) TLS や IPsec などで SIP 通信を保護する
TLS や IPsec などの暗号化プロトコル、トンネルプロトコルを利用して、SIP のヘッダの内容が盗聴されないようにする。

3) ID のあるなしで、違う応答をしないよう配慮する
SIP のリクエストに対して、ID や SIP アドレスが存在するかどうかに応じて異なる応答をしないよう配慮する。

4) 未認証リクエストの量や頻度の条件で、特定端末のリクエストをブロックする機能
未認証リクエストを連続して一定量送信する端末などを、ある条件で特定して、自動的にその端末からのリクエストを一定期間ブロックしつつ、記録(ログ)を残す機能も有用である。SIP サーバや SIP プロキシサーバならば実装しやすい。

19.4 参考情報

公開年月	情報源
2007 年 2 月	RSA Conference 2007 - Exploiting Voice over IP Networks http://www.hackingvoip.com/presentations/RSA%202007.pdf
2006 年 12 月	“Hacking VoIP Exposed – Voice over IP Security Secrets & Solutions”, David Endler and Mark Collier; McGraw-Hill Professional Publishing; ISBN: 0072263644 http://www.hackingexposedvoip.com/
2003 年	DefCon 11 – Watching the Watchers Target Exploitation via Public Search Engines http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Long/dc-11-long.ppt インターネット検索エンジンを利用して、秘密であるはずの情報を検索できてしまう問題と事例紹介。
2007 年 6 月	A Framework for Reducing Spam for Internet Telephony http://www.tschofenig.com/svn/draft-tschofenig-spit-prevention-framework/draft-tschofenig-sipping-framework-spit-reduction-00.txt
2006 年 12 月	Hacking VoIP Exposed - David Endler and Mark Collier for BlackHat 2006 http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Endler.pdf

【 項目 19. 登録 ID と構成情報の収集に関する問題 】

2010 年 7 月	5060/UDP に対するアクセスの増加について http://www.npa.go.jp/cyberpolice/detect/pdf/20100714.pdf UDP の 5060 ポートに対するアクセスが急増しているという警察庁からの報告。使用されたのは OPTIONS メソッドで、情報収集が目的と推測されている。

【 項目 20. SIP における TLS の不適切な利用から起こる問題 】

項目20. SIP における TLS の不適切な利用から起こる問題

20.1 概要

TLS を実装して利用する場合、適切に利用しないと、保護の効果が失われ、攻撃者によって成りすましをされ、TLS 暗号セッションに介入されることがある。その他 TLS の利用上の注意点をまとめる。

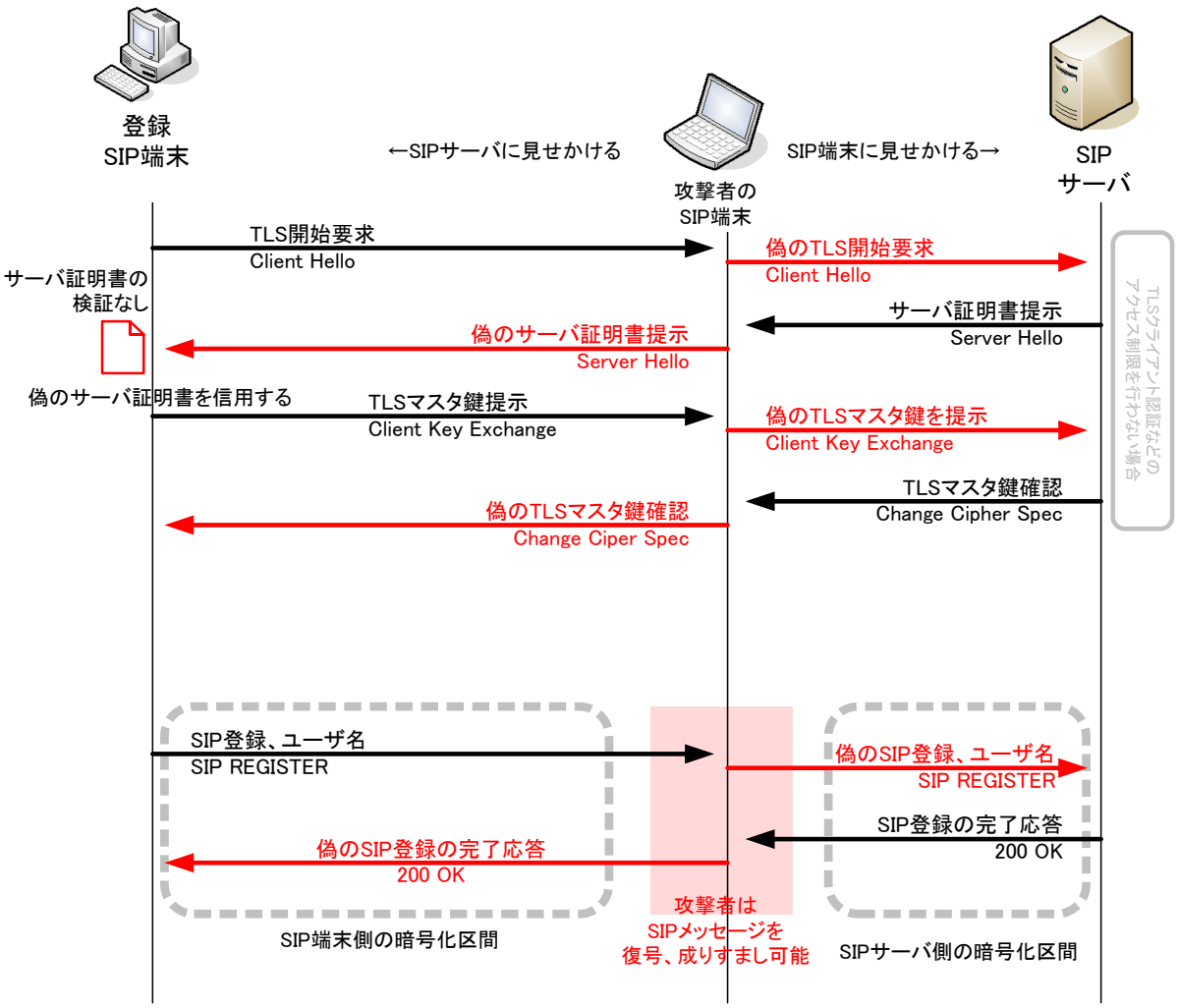


図 20-1 TLS 接続での成りすましと第三者による介入

20.2 解説

【攻撃手法とその影響】

TLS には、いくつかの攻撃手法があるが、そのうち、不正なサーバ証明書を利用して TLS 接続でなりすましを行い、第三者として暗号セッションに介入する攻撃についてとりあげる。このような第三者による介入は「Man in the Middle(MITM)攻撃」や「中間攻撃」あ

【 項目 20. SIP における TLS の不適切な利用から起こる問題 】

るいは「第三者介入攻撃」などと呼ぶ。

図 20-1 は TLS の暗号セッションを SIP 端末と SIP サーバの間で確立しようとしたが、攻撃者によって割って入られ、介入されてしまった状況を示している。

SIP 端末は TLS 接続を開始するため、SIP サーバに対して TLS 接続要求を送信するが、攻撃者は ARP 偽装や DNS 応答偽装などの手法を利用して SIP サーバに成りすまして、SIP 端末と攻撃者の間で TLS 暗号セッションを確立する。

一方、攻撃者は SIP サーバ側に対して、SIP 端末に成りすまし、TLS 暗号セッションを確立する。

攻撃者は TLS 暗号セッションに介入することで、SIP 端末と SIP サーバのそれぞれの通信内容を入手することができ、両方に対して成りすますことができる。そのため、図 20-1 の例では、TLS 暗号セッションに介入されたあと、SIP 端末が SIP サーバに送信した SIP REGISTER メッセージとその中に含まれるユーザ名が復号されて攻撃者の手に渡り、そのまま SIP サーバに成りすまして送信されている。その後交換される、SIP サーバからのチャレンジ文字列や、SIP 端末からのチャレンジ応答についても同様に攻撃者の手にわたることになる。

【原因と考察】

1) 公開鍵証明書の不適切な利用

TLS では、安全に暗号セッションを確立するために、公開鍵証明書を利用するが、図 20-1 の成りすましの例では、公開鍵証明書が適切に利用されないときに起こる。公開鍵証明書が適切に利用されていない例は次のものがある。

① SIP 端末が SIP サーバのサーバ証明書が正しい証明書か、検証していない
② SIP 端末が SIP サーバのサーバ証明書を検証して、不正な証明書だと判明しても、攻撃者のサーバ証明書を受け入れて TLS 暗号セッションを確立したとき
③ SIP 端末に、ニセの CA 証明書が注入されてしまっている
④ その他、公開鍵証明書の不適切な利用、運用

【 項目 20. SIP における TLS の不適切な利用から起こる問題 】

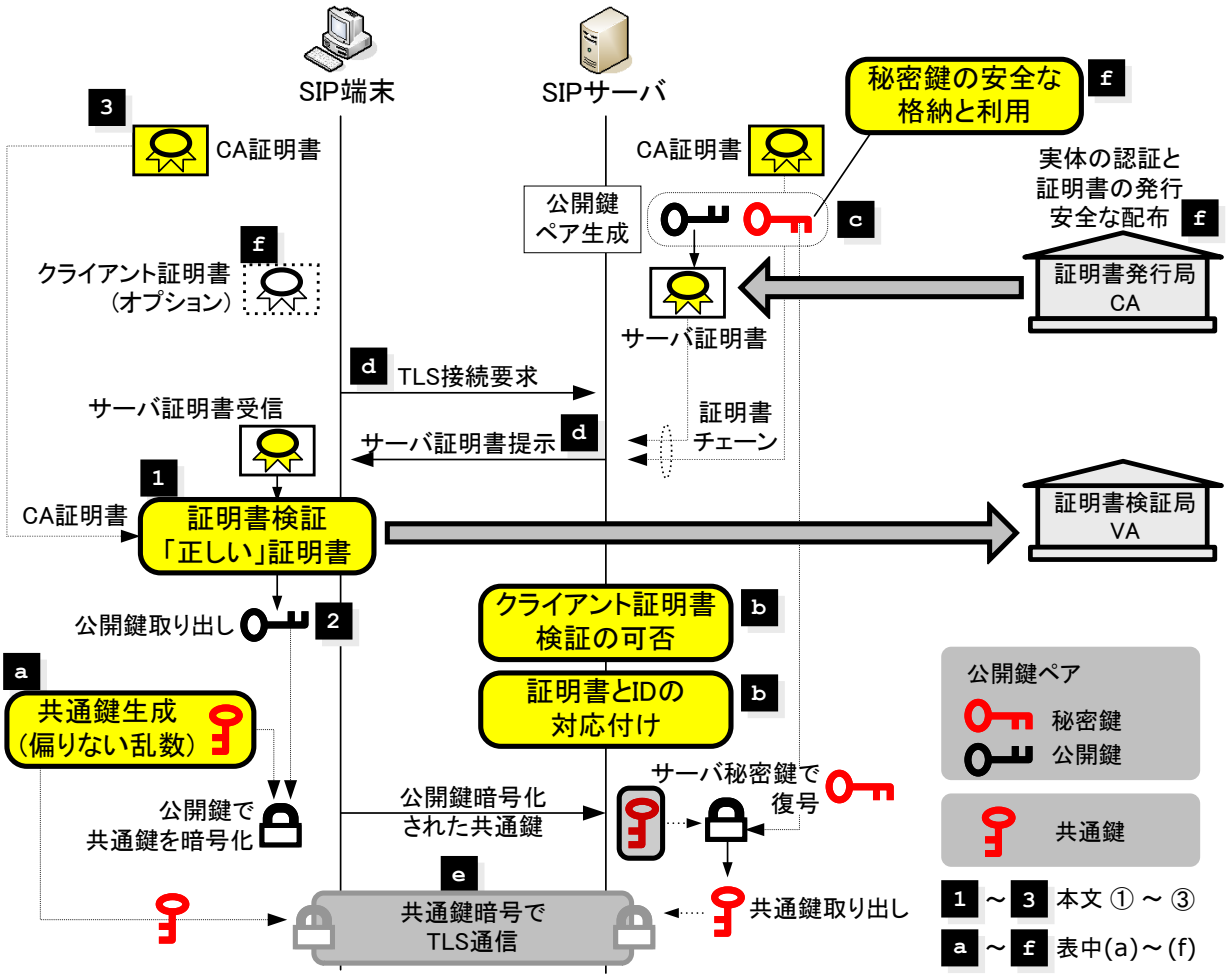


図 20-2 公開鍵証明書を利用した検証の手順と問題点

図 20-2 は、公開鍵証明書を利用した TLS サーバの検証と、TLS 暗号セッションを確立するまでの手順の概要を示している。①から③の例について、手順の概要を見ながら確認していく。

①SIP 端末が SIP サーバのサーバ証明書を検証しない場合と②SIP 端末が攻撃者のサーバ証明書をそのまま受け入れてしまう場合、SIP 端末は攻撃者が提示した不正なサーバ証明書を拒否しないため、そのまま TLS 暗号セッションを確立してしまう。図 20-2 左で、サーバ証明書受信のあと、CA 証明書を使って検証をする処理が行われないのと等しい。

③SIP 端末にニセの CA 証明書が注入されてしまっている場合、本来ならば端末には正しい CA 証明書だけがインストールされているはずである。図 20-2 の左上、SIP 端末内の CA 証明書は、サーバ証明書を検証するのに利用する。そのため、利用する予定のサーバ証明書を発行する CA の CA 証明書だけがインストールされていなければならない。もし第三者の、攻撃者のサーバ証明書を発行した CA の CA 証明書が SIP 端末内に注入されてしまうと、攻撃者のサーバ証明書が SIP 端末内で正しいサーバ証明書として検証されてしまう。

その他の公開鍵証明書の不適切な利用、運用については基本的に証明書の運用方針が不明確であることや、証明書の運用方針自体に間違いが含まれていることが挙げられる。例えば、一部の認証局(CA)が発行したサーバ証明書は、そのサーバ証明書に書かれている組織や会社名の実在証明が不十分で、証明書の信憑性が不十分である場合である。また、特定の CA が発行する証明書には、特定の目的や用途が指定されているため、安易に想定外の

用途に使うべきではない、などである。

こうした、公開鍵証明書の運用方針の策定の手順や解釈の方法については、「RFC 3647 インターネット X.509 PKI： 証明書ポリシーと認証実施フレームワーク(日本語)」が詳しい。

2) その他 TLS の不適切な実装と利用方法

その他の TLS の不適切な実装と利用方法について、一覧をまとめておく。2008 年 9 月現在、TLS のバージョンは 1.2 が最新である。過去のバージョンでは、複数の脆弱性に対応するなどの対策が行われているため、最新のバージョンを利用することが望ましい。

表 20-1 TLS の不適切な実装例、利用例

不適切な実装例、利用例	問題点	参照資料
(a)脆弱な乱数生成器を利用すること	TLS の暗号セッションで利用する共通鍵は乱数から生成するが、脆弱な乱数生成器は予測可能な乱数などを生成し、共通鍵暗号が解読される。	TLS 1.2 Appendix D.1
(b)証明書の検証を適切に行わない	証明書を適切に検証しないと、成りすましを許したり、機密情報が第三者に漏洩する。	TLS 1.2 Appendix D.2
(c)適切な強度の暗号方式を使っていない	匿名の Diffie-Hellman 方式では成りすましを許す。弱い鍵長は暗号を破られる。	TLS 1.2 Appendix D.3
(d)実装上のよくある間違い	TLS レコードが複数のフラグメントに分かれたときに適切に処理しているか？ ServerHello より前に届いた TLS バージョン番号はすべて無視しているか？ など	TLS 1.2 Appendix D.4
(e)暗号化方式に DES か IDEA を利用してしまう	DES 暗号は充分容易に解読されることが実証され、脆弱である。IDEA は実装例がほとんどないため脆弱である。	draft-ietf-tls-des-idea
(f)証明書の発行と検証に十分な安全性がない	証明書の発行、廃棄、検証を行うシステムや組織について、想定される脅威に対して必要十分な安全性が確保されないと、特定の攻撃に脆弱であったり、ムダな費用をかけてしまうことがある。使い勝手や性能、運用上の課題も多い。	「電子証明書と認証局」(@IT)

20.3 対策

【運用ガイド】

1) TLS で利用するサーバ証明書、その他証明書の運用方針を明確にして、文書化と共有、再確認の手順を常時行う。TLS 関連の証明書の運用方針には、守るべき対象と証明書の発行対象、証明書の利用目的、実在確認のレベル、利用する認証局(CA)、運用者の役割、証明書の導入・更新・廃止手順、検証が失敗したときの対応などがある。[RFC 3647]

【 項目 20. SIP における TLS の不適切な利用から起こる問題 】

【実装ガイド】

1) TLS を独自に実装する場合は、対象となるリスクの評価と対応策をよく検討する。実装にあたっては、RFC 5246 TLS 1.2 の標準仕様のほか、実装上の注意点、Appendix D. Implementation Notes もよく確認する。後方互換性について、セキュリティ上の検討事項についても、Appendix E, F がそれぞれ参考にする。
また、TLS の実装には、乱数の生成処理、ASN.1 データ形式の扱いや、AES などの暗号処理、SHA1 などのハッシュ関数の実装を利用することになるため、これらの機能も適切に実装または導入する必要がある。
2) 製品内部の TLS の機能、動作について、利用者が確認できるようにすること。具体的には実装ソフトのバージョン番号や、対応規格名、動作の概要説明資料などである。
3) 製品内部の TLS の機能は、実装の脆弱性や問題が判明したあと、なんらかの方法で更新できる実装が望ましい。

【 項目 20. SIP における TLS の不適切な利用から起こる問題 】

20.4 参考情報

公開年月	情報源
2003 年 10 月	CA-2003-26 Multiple Advisories in SSL/TLS Implementations http://www.lac.co.jp/info/cert_advisory/ca-2003-26.html ASN.1 ライブラリの問題による OpenSSL, SSLeay の脆弱性の問題
2003 年 11 月	RFC 3647: インターネット X.509 PKI: 証明書ポリシーと認証実施フレームワーク(日本語) http://www.ipa.go.jp/security/rfc/RFC3647JA.html (原文) RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://tools.ietf.org/html/rfc3647 証明書運用方針を計画するときの基本的な項目、手順など
2006 年 4 月	RFC4347 Datagram Transport Layer Security (DTLS) http://www1.tools.ietf.org/html/rfc4347
2006 年 9 月	Peer Authentication Vulnerability In Ingate Products (SIP Over TLS - X.509) http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-09/msg00023.html exponent 65535 ではなく、exponent 3 を利用する公開鍵証明書では TLS を乗っ取られることがある問題
2007 年 5 月	JVNDB-2007-000404 RSA BSAFE Cert-C および Crypto-C にサービス運用妨害 (DoS) の脆弱性 http://jvndb.jvn.jp/ja/contents/2007/JVNDB-2007-000404.html Cisco Security Advisory: Vulnerability In Crypto Library Document ID: 91890 Advisory ID: cisco-sa-20070522-crypto.shtml http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml TLS 内でも利用している ASN.1 実装の脆弱性により、複数のセキュリティ機能に脆弱性が及んだ例
2010 年 5 月	RFC5763 - Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS) 6.9. Media over SRTP http://tools.ietf.org/html/rfc5763#section-6.10
2008 年 4 月	iSkoot disclosure of Skype credentials resolved http://voipsa.org/blog/2008/04/28/iskoot-disclosure-of-skype-credentials-resolved-new-version-by-wednesday/ Skype 対応の Symbian 端末で、Skype の秘密鍵が読み取れると指摘した問題
2008 年 5 月	AST-2008-007 Cryptographic keys generated by OpenSSL on Debian-based systems compromised http://voipsa.org/pipermail/voipsec_voipsa.org/2008-May/002671.html Debian Linux 用の Asterisk で、OpenSSL で実装された乱数生成器が脆弱だった問題
2008 年 8 月	RFC 5246 The Transport Layer Security (TLS) Protocol, Version 1.2 http://tools.ietf.org/html/rfc5246 TLS の最新仕様。注意点、補足情報も豊富
2008 年 6 月	Datagram Transport Layer Security version (DTLS) 1.2 http://tools.ietf.org/html/draft-ietf-tls-rfc4347-bis 2010 年 7 月にドラフト 04 が公開

【 項目 20. SIP における TLS の不適切な利用から起こる問題 】

随時更新	IETF TLS Working Group http://www.ietf.org/html.charters/tls-charter.html TLS 仕様の拡張、補足仕様に関する最新仕様と提案
随時更新	IETF PKIX Working Group http://www.ietf.org/html.charters/pkix-charter.html X.509 公開鍵インフラのワーキンググループ。証明書の属性、証明書失効リストの形式とオンライン検証プロトコル、証明書管理メッセージなどの標準化と提案

20.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	■ Ⅰ （注意）	□ Ⅱ （警告）	□Ⅲ （危険）
本脆弱性の CVSS 基本値	2.6		

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	■高	□中	□低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響 （情報漏えいの可能性）	□なし	■部分的	□全面的
完全性への影響 （情報改ざんの可能性）	□なし	■部分的	□全面的
可用性への影響 （業務停止の可能性）	■なし	□部分的	□全面的

【 項目 21. SRTP の暗号に用いる共通鍵が盗聴される問題 】

項目21. SRTP の暗号に用いる共通鍵が盗聴される問題

21.1 概要

項目 8 で示したように、攻撃者によって RTP パケットを盗聴される環境では、RTP 上のメディアストリームを保護する方法のひとつとして、SRTP(Secure RTP)を利用することができる。SRTP では、メディアストリームの暗号化のための共通鍵(以下、共通鍵)を、SIP メッセージ上にある SDP 内で交換する。

SIP メッセージ上の SDP 内で SRTP 用の共通鍵を交換するとき、実装によっては共通鍵そのものが生のテキストで記述されていることがある。この場合、SIP メッセージを盗聴できる環境では、SRTP 用の共通鍵を攻撃者が容易に入手でき、暗号化されたメディアストリームの内容が攻撃者によって解読されたり、改ざんされる可能性がある。

21.2 解説

【攻撃手法とその影響】

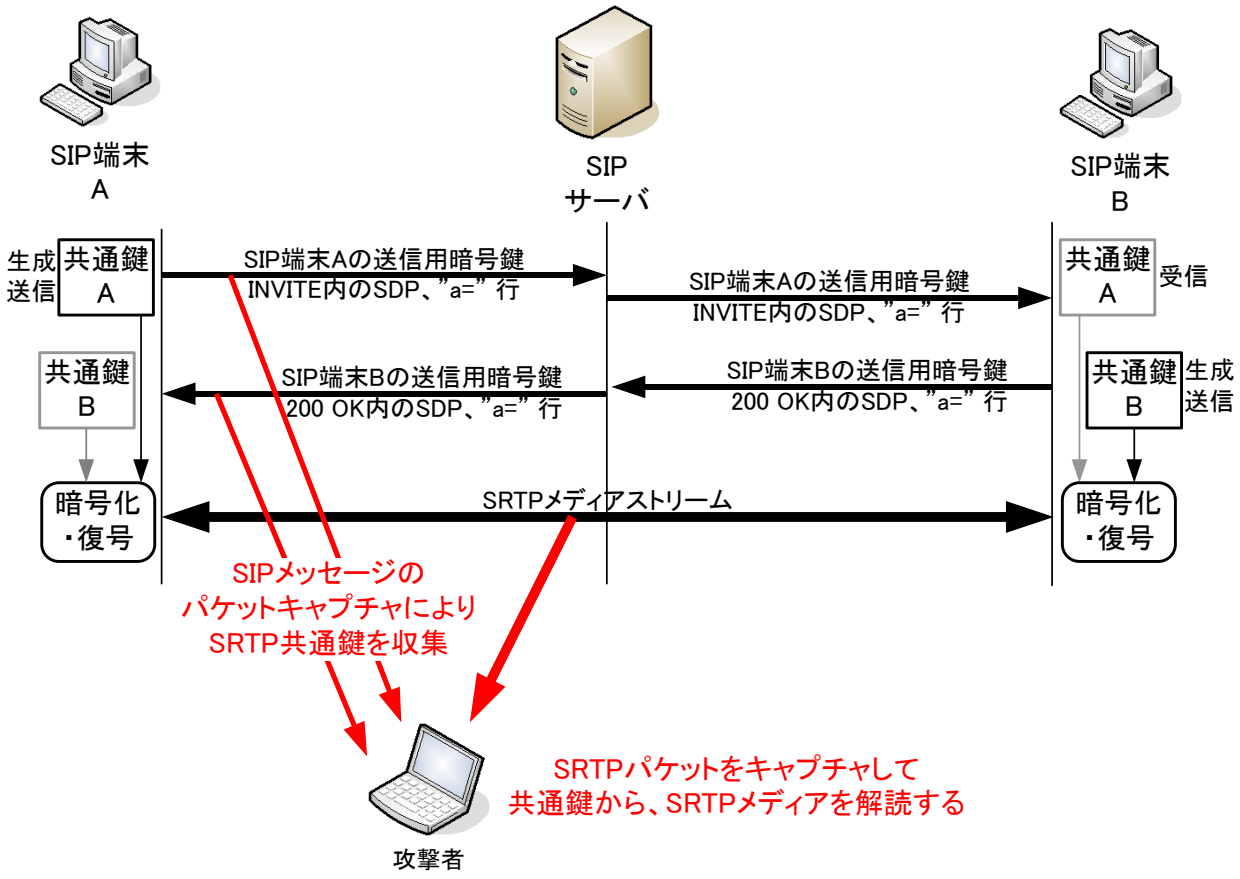


図 21-1 SIP 上での SRTP 共通鍵交換と、SRTP メディアストリームの盗聴、解読

【 項目 21. SRTP の暗号に用いる共通鍵が盗聴される問題 】

攻撃者は通信路上で、他のホストのパケットを取り出せる環境で、まず攻撃対象の SIP 端末が送受信する SIP メッセージを含む IP パケットのキャプチャを行う。

この中から、INVITE メッセージと 200 OK 応答に含まれる SDP を取り出し、さらに a=crypt 行で始まる、暗号鍵の記述を取り出して、送受信者のそれぞれの SRTP 用の暗号鍵をとりだす。a=crypt 行で始まる暗号鍵の記述例を図 21-2 に示す。各行はそれぞれ 1 行で記述するが、長い行は改行したあと、先頭に空白を挿入して連続行としてみなしている。この例は RFC 4568 の例だが、a=crypt 行が 2 行あり、最初の行はビデオのメディアストリーム用の暗号鍵が、次の a=crypt 行は音声のメディアストリーム用の暗号鍵が記述されている。

```
v=0
o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.example.com/seminars/sdp.pdf
e=j.doe@example.com (Jane Doe)
c=IN IP4 161.44.17.12/127
t=2873397496 2873404696
m=video 51372 RTP/SAVP 31
a=crypto:1 AES_CM_128_HMAC_SHA1_80
 inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
m=audio 49170 RTP/SAVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_32
 inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32
m=application 32416 udp wb
a=orient:portrait
```

図 21-2 共通鍵を含む SDP メッセージの例（RFC 4568）

その後、SRTP のメディアストリームが確立されたら、さきほど取り出しておいた SRTP 用の暗号鍵を使って、SRTP メディアストリームをキャプチャしながら解読し、メディアストリームの内容を盗聴する。

SRTP メディアストリームの盗聴による被害は、RTP メディアストリームの盗聴による被害とほぼ同様である。例えば、IP 電話の通話中の会話、IP 電話で音声自動応答システム(IVR)などに入力するプッシュ番号、テレビ会議でのビデオカメラの映像やアプリケーションの画面例、などが攻撃者に知られることにつながる。ただし、一般的に SRTP で保護するようなメディアストリームの内容は、RTP だけを使う場合に比べると、よりリスクが高いコンテンツであると考えられる。

また、RTP パケットには、RTP を制御するための、RTCP(リアルタイム制御プロトコル: Realtime Control Protocol)の情報も含まれているため、RTP メディアと同様に、RTP の品質レポートや RTP の発信者情報なども露出する。RTCP の詳しい内容については「[参照]10. RTCP の偽装から起こる問題」を参照されたい。

【原因と考察】

1) 鍵交換の保護は RFC4568 SDES 仕様の範囲外

SRTP[RFC3711]は音声やビデオのようなリアルタイムなメディアストリームの転送処理のために、RTP パケットのうち、保護する対象をできるかぎり最小限にとどめた方式である。IPsec では最大で、IP パケット全体が暗号化されるが、SRTP では RTP ペイロード

【 項目 21. SRTP の暗号に用いる共通鍵が盗聴される問題 】

のみが暗号化される。

SRTP の問題は、暗号化やメッセージ署名に使う、暗号鍵の交換方法を定めていない、という点である。そこで、RFC 4568 では、SRTP に限らず、メディアストリームで利用する暗号化やメッセージ署名のための共通鍵を交換するために、SDP に暗号方式や鍵データを記述する手順を標準化している。SIP メッセージ内の SDP 上に"a="属性の値として記述され、a=crypt 行として記述される。この方法を業界では"sDescription(SDES)での鍵配布"などと呼ぶ。

しかし RFC4568 では、SRTP 用の暗号鍵の保護は RFC4568 仕様の範囲外であり、SDP 内の暗号鍵はバイナリデータをテキスト形式に変換して記述しているだけである。そのため、第三者が SDP 上に記述された暗号鍵を、SIP メッセージを盗聴するなどして入手すれば、簡単にバイナリデータに復号でき、SRTP で暗号化されたメディアストリームを解読するために再利用できてしまう。

2) SRTP 用鍵交換の保護

SRTP のための鍵交換を保護する対策としてはいくつかの方法がある。まず、SDP を含む、SIP メッセージ全体を TLS や IPsec などで保護する方法がある。また、SIP メッセージのヘッダを除く、ボディ部分だけを暗号化する S/MIME で SDP 全体を保護する方法もある。また、SDP のうち鍵交換の処理だけを、MIKEY や ZRTP、IKE などで処理する方法もある。それぞれの利点と問題は以下の表 8 のようになる。ここで共通の条件にしているのは、SRTP の暗号鍵交換を保護するためには、SRTP のメディアストリームを確立する端末間で直接行う必要がある、という点である。

表 8　SRTP 用の鍵交換を保護する方法

保護方式	保護の対象範囲	利点	問題
TLS	SIP メッセージすべてを含む通信路全体	SIP 環境でよく普及している	IP-PBX など、端末間に介入する呼制御サービスを提供できない
IPsec		インターネット環境で一定の普及がある	
S/MIME	SIP のボディ部分にあたる SDP の全体	テキスト形式	
MIKEY	SRTP の鍵のみ	短時間で処理するために 1 往復だけで完了させる	時刻同期がないとリプレイ攻撃に弱い
ZRTP		RTP メディアストリームをすぐに開始できる	RTP の初期段階を保護できないことがある
IKE		IPsec での実績がある	SIP 環境では普及していない

上の表 8 にある、SRTP 用の鍵交換の保護については、SIP との間で目的のズレがある。SIP は柔軟な呼制御を提供するため、SIP 端末の間に SIP サーバや SIP プロキシが介在して、セッションの転送や保留、認証や課金、複製や変換などさまざまな仲介処理を行う。一方、SRTP は SIP による呼設定が終わったあとで確立する、1 対 1 の対向通信であり、仲介処理は SIP ほど必要ではない。そのため、SRTP では端末間でのエンドツーエンドの暗号鍵の交換が必要になる。

このように RTP メディアストリームの保護を重視する場合は対向でのエンドツーエンドの鍵交換と暗号化が必要になり、SIP の柔軟な呼制御機能を重視する場合は SIP サーバを介したホップバイホップの処理を可能にするため、SRTP の鍵交換は SIP とは独立して処理することが理想になる。

【 項目 21. SRTP の暗号に用いる共通鍵が盗聴される問題 】

そこで、TLS の UDP 拡張である DTLS(RFC 4347: Datagram Transport Layer Security)を利用して、SIP とは独立に、安全に生成・交換された鍵を SRTP のための暗号鍵として使う標準仕様が DTLS-SRTP として提案されている。

※ Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)
http://tools.ietf.org/html/rfc5764

DTLS-SRTP では、よく普及して長年の実績がある TLS を利用して、安全に鍵を生成する。その上で SRTP の対向にあたるホスト間で安全に鍵を交換し、SRTP の暗号鍵を生成する手順である。DTLS だけでメディアストリームを暗号化するには処理が重すぎるため、DTLS は鍵の生成と交換の処理までに限定されている。そのあとのメディアストリームの暗号化処理はパケット数が多いため SRTP に処理させている。DTLS-SRTP はまた、SRTP の鍵交換を保護するが、SIP 自体の保護は行わず、別の方法を利用する前提となっている。このような SIP と RTP の保護を個別に独立して考え、分担させる方法については、DTLS-SRTP framework(RFC 5763: Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS))としてまとめられている。

21.3 対策

【運用ガイド】

1) 攻撃者の盗聴用のホストが SIP、SRTP と RTP を利用するネットワークに接続できないように、SIP を利用するネットワークを VLAN や別の物理ネットワークに隔離する。
2) または追加の暗号化通信装置を利用して、SIP の通信を TLS や DTLS、IPsec などで保護する。

【実装ガイド】

1) RTP メディアストリームを確立するときに、SRTP 用の暗号鍵を交換する場合は、ネットワーク上で容易に暗号鍵を取り出せないようにする。そのために、SIP を TLS や DTLS、IPsec など別の暗号化通信方式で保護する。
2) IPsec を利用する場合、アプリケーションやシステムの SIP/RTP を利用する機能モジュールからは IPsec の制御が直接できない場合があるため、実装方法や利用手順には注意が必要だ。

【 項目 21. SRTP の暗号に用いる共通鍵が盗聴される問題 】

21.4 参考情報

公開年月	情報源
2003 年 7 月	RFC3550 RTP: A Transport Protocol for Real-Time Applications(最新版) 9. Security http://tools.ietf.org/html/rfc3550
2004 年 3 月	RFC3711 The Secure Real-time Transport Protocol (SRTP) http://tools.ietf.org/html/rfc3711
2006 年 4 月	RFC4347 Datagram Transport Layer Security (DTLS) http://tools.ietf.org/html/rfc4347 *一部修正(Erratta) http://www.rfc-editor.org/errata_search.php?rfc=4347
2008 年 7 月	DTLS-SRTP Key Transport http://tools.ietf.org/html/draft-wing-avt-dtls-srtp-key-transport
2010 年 5 月	RFC5764 - Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP) http://tools.ietf.org/html/rfc5764
2010 年 5 月	RFC5763 - Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS) http://tools.ietf.org/html/rfc5763

21.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	□ I （注意）	■ II （警告）	□III （危険）
本脆弱性の CVSS 基本値		5.0	

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	□高	□中	■低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響 （情報漏えいの可能性）	□なし	■部分的	□全面的
完全性への影響 （情報改ざんの可能性）	■□なし	□部分的	□全面的
可用性への影響 （業務停止の可能性）	■なし	□部分的	□全面的

【 項目 22. 暗号化された SRTP が共通鍵なしで解読される問題 】

項目22. 暗号化された SRTP が共通鍵なしで解読される問題

22.1 概要

VBR(Variable Bit Rate: 可変ビットレート)で音声メディアを符号化または圧縮すると、SRTP(Secure RTP)で暗号化したとしても、個々のパケットの長さの違いと送出パターンを分析することで、SRTP 用の共通鍵がなくても元の音声(2008 年時点で英単語)を解読される可能性がある問題。

22.2 解説

【攻撃手法とその影響】

他のホストのパケットを取り出せる環境で、SRTP メディアストリームを含む IP パケットのキャプチャを行う。キャプチャしたパケットから、音声の SRTP メディアストリームを特定する。

音声メディアストリームが VBR(Variable Bit Rate: 可変ビットレート)で符号化または圧縮されている場合、それぞれのパケットの長さと、パケットの送出パターンについて、事前に作成しておいた送出パターンの辞書と照らし合わせながら分析することで、発声された単語を予想する。

2008 年 3 月の[VBR 解析]によれば、この方法による音声の解読の成功率について、特定の英単語については 90%以上解読できるとされている。その他を含めた会話全体については約 50%の解読率とされている。今後、解読率を向上させていくためには、特定話者の業務内容や専門分野に適応した辞書を作成し、利用する必要がある、と指摘されている。

この、VBR のパケット送出パターンによる音声解析は、RTP メディアの暗号化、復号のための鍵をまったく必要としない。そのため、暗号化の前後でパケット長が同じになるような暗号化方式では、暗号化によるデータの保護がまったく意味を持たない点が重要である。

【原因と考察】

RTP では、音声やビデオなどのメディアストリームはすべて、デジタル化された信号で転送される。デジタル化するためには、なんらかの符号化を行う。例えば、マイクで収集した信号は、音声アナログ信号だが、これを G.711 という符号化方式を利用すると、アナログ信号に対して毎秒 8,000 回、8 ビットの符号でデジタルの値に変換を行う。このような G.711 の PCM 符号化では、毎秒 64Kbps の、符号化されたデータが得られるため、固定ビットレート(CBR: Constant Bit Rate)と呼ばれる。

VBR は、音声やビデオなどのアナログ信号をデジタル信号に符号化するとき、常に同じビットレートではなく、元のアナログ信号の特徴に応じた、可変長のビットレートで符号化または符号化後に圧縮する方法である。JPEG や MPEG などでは、人が色や音を認識するときに、細かく判別できる色域や音量に偏りがあることを利用しているため、圧縮後のデータ量を可変にできる。

RTP での音声符号化と圧縮では、特に人の会話に最適化されている方法の場合、人体の声帯のふるわせ方や、口の発音の動作から、音声の特徴を抽出する符号化が行われている。このような音声符号化方式には、CELP(Code-Excited Linear Prediction)がある。CELP は音声の特徴をコードブックという辞書に持ち、音声データから辞書に含まれるデータを符号の形で抽出して圧縮する。CELP は人体に共通な音響的な特徴を辞書に持つことによって、特定の国や地域の言語には関係なく圧縮効果を得ることができる。

また、CELP 方式では、音声の特徴を整理した辞書内の項目数が多ければ音声の詳細度

が高くなり、ビットレートが高くなる。その反対に、辞書内の項目数が少なければ、音声の詳細度が低くなり、ビットレートも低くなる。特に CELP の派生方式である QCELP と Speex は VBR 方式を採用しており、音声品質を向上するために発音の種類に応じて高速に音声符号化のビットレートを変化させている。

また、会話や単語の間の、断続的に細かく声が途切れる状況に対しても、符号化データを削減したり、音声データを生成しない処理(VAD: 発話区間検出)が行われている。

こうした VBR に対応した音声符号化や圧縮と、無音の処理によって、単語や会話は音声データにしたときにパケット長とパケット数が大きく異なることになる。こうしたパケット長とパケット数の変化は元の発音や会話を予想するのに利用できる。

こうした VBR ビットレートの解析を実際に行い、特定の英単語について 90%解読できた、とする論文が、[VBR 解析]である。

従来、このようなトラフィックパターンによる解析は Winny や Skype のような暗号通信を利用する P2P ファイル交換トラフィックの発見や抽出に利用される事例があった。音声についてはさらに短いパケット長で、多数のパケットに対して、より面的なパケット量分析が行われている。

22.3 対策

【運用ガイド】

1) 音声信号を SRTP で暗号化する場合は、音声符号化や音声圧縮方法に VBR を利用せず、固定ビットレート(CBR)での符号化方式を利用する。
2) 音声信号を SRTP で暗号化するとき、音声を VBR 符号化すると、音声を解読される可能性があることを利用者に示す。

【実装ガイド】

1) SRTP で VBR を利用するときに、送出側でパケット長を撹乱するためのパディングデータを挿入または追加する。受信側でもパディングデータへの対応を行う。
2) VBR で符号化または圧縮をするとき、ある程度の周辺雑音も含めた符号化または圧縮を行い、もとの音声の特徴が表れにくくする。
3) SRTP で RTP を暗号化するとき、音声の VBR 符号化を選択できないようにする。

【 項目 22. 暗号化された SRTP が共通鍵なしで解読される問題 】

22.4 参考情報

公開年月	情報源
2003 年 7 月	RFC3550 RTP: A Transport Protocol for Real-Time Applications(最新版) 9. Security http://www1.tools.ietf.org/html/rfc3550
2004 年 3 月	RFC3711 The Secure Real-time Transport Protocol (SRTP) http://www1.tools.ietf.org/html/rfc3711
2007 年 4 月	Asterisk encryption http://www.voip-info.org/wiki/view/Asterisk+encryption Asterisk で SRTP を利用するための設定、互換機器・ソフトなど。
2008 年 3 月	[VBR 解析] " Uncovering spoken phrases in encrypted VoIP conversations" Johns Hopkins University, Department of Computer Science http://www.cs.jhu.edu/~fabian/papers/oakland08.pdf 暗号化 VoIP 通話から、発声単語を解読する手法を紹介した論文。VBR 時のパケット長、パケット数の変化を高速に解析した事例グラフや図版が豊富。その他、パケット長からの単語の予測を行うための辞書の機械的な学習手法や、前後の単語からの解析手法も検討しており、手法が洗練されている。
2008 年 6 月	MIT Technology Review - Breaking Phone-Call Encryption http://www.technologyreview.com/Infotech/20913/?a=f VBR 解析論文の解説、VoIP メーカ技術者のコメントなど。 MIT Technology Review はマサチューセッツ工科大学所有の Technology Review 社が発行する、世界最古(1899 年)と言われる技術評論誌。

【 項目 22. 暗号化された SRTP が共通鍵なしで解読される問題 】

22.5 CVSS 深刻度評価(参考値)

【評価結果】

本脆弱性の深刻度	□ Ⅰ（注意）	■ Ⅱ（警告）	□Ⅲ（危険）
本脆弱性の CVSS 基本値		5.0	

【CVSS 基本値の評価内容】

攻撃元区分	□ローカル	□隣接	■ネットワーク
攻撃条件の複雑さ	□高	□中	■低
攻撃前の認証要否	□複数	□単一	■不要
機密性への影響 （情報漏えいの可能性）	□なし	■部分的	□全面的
完全性への影響 （情報改ざんの可能性）	■なし	□部分的	□全面的
可用性への影響 （業務停止の可能性）	■なし	□部分的	□全面的

用語集

用語	説明
3GPP	3rd Generation Partner Project：第 3 世代携帯電話の標準化組織
ACK	SIP における「セッション確立」要求メッセージ
AES	Advanced Encryption Standard：米国商務省標準技術局(NIST)によって選定された次世代標準暗号化方式
AIPN	All IP Network：サーバ、端末も含めて、すべて IP プロトコルで構成されたネットワーク。
AJAX	Asynchronous JavaScript + XML：JavaScript の HTTP 通信機能を使った対話型 Web アプリケーションの実装形態
ARP	Address Resolution Protocol：IP アドレスから Ethernet アドレス（MAC アドレス）を検索するためのプロトコル
ARP Poisoning	MAC アドレスを偽ってネットワークに侵入する攻撃手法
ARP Spoofing	送信元 IP アドレスを偽ってネットワークに侵入する攻撃手法
ASCII 文字	半角の英数字や記号などの ASCII コードで表現される文字。日本語文字や全角の英数字、記号などは含まれない。
BYE	SIP における「セッション終了」リクエストメッセージ
CA	Certificate Authority：PKI 環境で、暗号通信や署名、認証などに必要となる、電子証明書を発行する機関。
Call-ID	SIP リクエスト・レスポンスを識別するための ID
CANCEL	SIP における「未確立セッション取り消し」リクエストメッセージ
CELP	Code-Excited Linear Prediction：音声をデジタル符号化する方式の 1 つ
CNAME	Canonical Name：別名定義
CODEC、コーデック	符号化方式を使ってデータのエンコード（符号化）とデコード（復号）を双方向にできる装置やソフトウェア
Contact ヘッダ	当該メッセージ以降のリクエストの送信先を URI で指定するヘッダ
CSeq(値)	SIP リクエストの順序を示すための値
CVE	Common Vulnerabilities Exposures：非営利団体の MITRE Corporation によって管理・運営されている脆弱性リスト
CVSS	Common Vulnerability Scoring System：共通脆弱性評価システム
DCCP	Datagram Congestion Control Protocol：UDP 上での輻輳制御プロトコル
DDoS	Distributed Denial of Service：分散サービス妨害
DES	Data Encryption Standard：1960 年代後半に IBM 社によって開発された秘密鍵暗号化アルゴリズム
Diffie-Hellman	安全でない通信経路を使って秘密鍵を安全に送受信するための鍵交換方式
DNS	Domain Name System：インターネット上のホスト名と IP アドレスを対応させるシステム

用語	説明
DoS	Denial of Service：サービス拒否攻撃。攻撃対象に不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させてサービスを停止させる攻撃。
DTLS	Datagram Transport Layer Security：データグラムトランスポート層セキュリティ
DTMF	Dial Tone Multi Frequency：プッシュ方式の電話機などで、ボタン押すことで発信される音プッシュ音、トーン信号。
Ethernet	IEEE 802.3：Xerox 社と DEC 社が考案した LAN 規格
Firewall、FW、F/W	ファイアウォール。内部ネットワークをネットワーク外部から防御することを目的としたソフトウェアやハードウェア
From ヘッダ	リクエストの送信者を指定するヘッダ。同時に送信者を識別するための値である tag を設定する。
FTTH	Fiber To The Home：光ファイバーを用いた家庭向けのデータ通信サービス
Fuzzing	エラー成分が含まれた様々な命令パターンを実行させてエラーの発生を調べる手法。またはその手法を用いた攻撃。
G.711	ITU-T の音声符号化方式の勧告。PCM（パルス符号変調）方式により電話線上で 64kbps の伝送を実現する方式。
H.323	ITU-T の音声、映像方式、データ圧縮伸長方式の勧告。
HA	High Availability：高い可用性を実現する機能やシステム
hop-by-hop	パケットの転送経路途中の全中継点で実施されるべき処理
HTTP	Hypertext Transfer Protocol：Web サーバと Web ブラウザ間で HTML コンテンツの送受信に用いられる通信プロトコル
I/F	Interface、インターフェース
ICMP	Internet Control Message Protocol：TCP/IP プロトコルにおいて、その機能を補助する制御用プロトコル
ID	Identifier：識別子。対象を一意に識別する名前。
IPS	Intrusion Prevention System：不正侵入防御システム
IDS	Intrusion Detection System：不正侵入検知システム
IETF	The Internet Engineering Task Force：インターネットで利用される技術の標準化を策定する組織
IMS	IP Multimedia Subsystem
INFO	SIP における「セッション内での情報交換」リクエストメッセージ
INVITE	SIP における「セッション開始」要求メッセージ
IP	Internet Protocol：インターネットで情報伝達を行うプロトコル。OSI 参照モデルのネットワーク層にほぼ対応する機能を持つ。
IPsec	Security Architecture for Internet Protocol：インターネットで暗号通信を行なうための規格。IP パケットを暗号化して送受信する。
IP 電話	電話網の一部もしくは全てに VoIP 技術を利用する電話サービス

用語	説明
IVR	Interactive Voice Response：音声自動応答装置
JPEG	静止画像（デジタルデータ）の圧縮方式
JVN	Japan Vulnerability Notes：日本国内の製品開発者の脆弱性対応状況を公開するサイト
MAC アドレス	Media Access Control address：Ethernet などのデータリンク層で各ノードを識別するためのハードウェア固有の物理アドレス
MD5	Message Digest 5：ファイル改ざんの確認などに用いられるハッシュ関数(一方向要約関数)
MEGACO	media gateway control：通信事業者が IP ネットワーク上で電話サービスを提供する際に利用するプロトコルの一つ
MESSAGE	SIP における「メッセージ送信」リクエストメッセージ
MIB	Management Information Base：管理情報ベース
MIKEY	Multimedia Internet Keying：SRTP で利用される暗号鍵交換プロトコル
MITM	Man in the Middle：第三者介入攻撃、中間攻撃。
MPEG	Moving Picture Experts Group：映像データの圧縮方式の一つ
NGN	Next Generation Network：IP ネットワークをベースとした次世代の通信事業者のネットワーク
NOTIFY	SIP における「ユーザの情報伝達」リクエストメッセージ
NTP	Network Time Protocol：時刻同期プロトコル
OMA	Open Mobile Alliance：世界各国のモバイル通信関連企業の業界団体
PKI	Public Key Infrastructure：公開鍵暗号を用いた技術・製品・サービスの基盤。
PPPoA	PPP over ATM：PPP 接続を ATM ネットワーク上で利用するためのプロトコル
PPPoE	PPP over Ethernet：PPP 接続を Ethernet 上で利用するためのプロトコル
PRACK	SIP における「信頼性のある暫定レスポンス」リクエストメッセージ
PUBLISH	SIP における「状態情報の通知」リクエストメッセージ
QCELP	Qualcomm's Code Excited Linear Prediction：クアルコム社が CDMA 方式移動体電話システム用に開発した CELP 方式の一つ。
REFER	SIP における「転送」要求メッセージ
REGISTER	SIP における「contact アドレス登録」リクエストメッセージ
re-INVITE	セッションに関わるメディアフローの特徴を変更したり、SIP セッションタイマーを更新するために利用され
response	ダイジェスト認証で用いられる認証データの計算結果である値
RFC	Request For Comment：IETF による技術仕様
RLOGIN	リモートホストにログインするときに使用する UNIX コマンド

用語	説明
ROHS 指令	Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment：EU(欧州連合)が施行した電気電子機器への特定有害物質の含有を禁止する規制
RST フラグ	コネクションを強制的に切断するときなどに利用する TCP ヘッダ内の制御用フラグ
PSTN	Public Switched Telephone Networks：既存の一般公衆電話網のこと。IP 電話網や携帯電話網と対比して使う。
RTCP	RTP Control Protocol：RTP を利用する際にデータの送受信制御および送信者と受信者の情報を記述するプロトコル
RTP	Real-time Transport Protocol：音声や映像をストリーミング再生するための伝送プロトコル
S/MIME	Secure Multipurpose Internet Mail Extensions：電子メールの代表的な暗号化方式
SANS	米国のセキュリティ関連組織
SDP	Session Description Protocol
SHA	Secure Hash Algorithm 1：SHA1：認証やデジタル署名などに使われるハッシュ関数の一つ
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol：セッション開始プロトコル。
SIP UA	SIP User Agent：SIP ユーザエージェント
SIP URI、SIP-URL	SIP Uniform Resource Identifier：SIP 用に定められているアドレス指定形式。
SIP サーバ	SIP サービスを提供するサーバ
SIP メソッド	SIP におけるリクエスト(要求)メッセージ
SNMP	Simple Network Monitoring Protocol：ネットワーク管理プロトコル
SPAM	インターネットを利用したダイレクトメール、迷惑メール
Speex	主に会話を圧縮するための音声圧縮技術の一つ
SPIT	Spam for Internet Telephony：IP 電話を使った迷惑電話
SRTP	Secure Real-time Transport Protocol：音声や動画などのリアルタイム通信で用いられる RTP を暗号化する技術
SSL	Secure Socket Layer：TCP または UDP 上の通信を暗号化するプロトコル（TLS も参照）
SSL-VPN	Secure Socket Layer Virtual Private Network：暗号化に SSL を利用する VPN 技術
SSRC	Synchronization Source Identifier：同期ソース識別子
SUBSCRIBE	SIP における「ユーザの情報伝達要求」リクエストメッセージ
TCP	Transmission Control Protocol：トランスポート層のデータ伝送制御プロトコルの一つ。TCP は UDP に比べ信頼性は高いが転送速度が低い。
TCP/IP	Transmission Control Protocol/Internet Protocol：インターネットなどで使われている基本的な通信プロトコルである TCP と IP の複合的な呼称

用語	説明
TELNET	ネットワークにつながれたコンピュータを遠隔操作するための標準的なプロトコル
TFTP	Trivial File Transfer Protocol。
TLS	Transport Layer Security：TCP または UDP 上の通信を暗号化するプロトコル(→SSL も参照)。
To ヘッダ	リクエストメッセージの受信者を指定する
UA	ユーザエージェント。ユーザが利用する端末やソフトを指す。
UAC	User Agent Client：ユーザエージェントクライアント
UAS	User Agent Server：ユーザエージェントサーバ
UDP	User Datagram Protocol：トランスポート層のデータ伝送制御プロトコルの一つ。UDP は TCP に比べ転送速度は高いが信頼性が低い。
UOPF	Ubiquitous Open Platform Forum
UPDATE	SIP における「セッション情報の更新」リクエストメッセージ
URL	Uniform Resource Locator：インターネット上に存在するコンテンツの場所を特定する記述方式
VBR	Variable Bit Rate：可変ビットレート
Via	SIP のバージョン、データ伝送に使用するプロトコル、このリクエストに対するレスポンスはここへ送って欲しい旨通知
VLAN	Virtual LAN：物理的な接続形態とは独立した仮想的なネットワークグループ
VoIP	Voice over IP：音声を符号化方式で圧縮とパケットへの変換行い、IP ネットワークでリアルタイム伝送する技術
VRRP	Virtual Router Redundancy Protocol：仮想的ルータ冗長プロトコル
Web	World Wide Web の略称
WEP	Wired Equivalent Privacy：無線通信における暗号化技術の一つ
WPA	Wi-Fi Protected Access：WEP の弱点を補強し、セキュリティ強度を向上させた無線通信における暗号化技術
X.509	電子鍵証明書および証明書失効リスト(CRL)の標準仕様
ZRTP	電子メールの暗号化方式である PGP を開発した Phil Zimmerman(フィル・ジンマーマン)が提案する RTP の保護方式
シーケンス	連続した一連の手順
シグナリング	通信を接続したり切断するための呼制御
ダイアログ ID	To ヘッダ、From ヘッダ、および Call-ID を組み合わせたもの
ダイジェスト認証	パスワードから生成されるダイジェスト(一方向ハッシュ関数にデータを入力することで得られる値)のみを使う認証方式
バックドア	不正侵入を行なうための「裏口」
ブロードキャストアドレス	ネットワーク内の全ての端末にデータを送信するために使われる特殊なアドレス

用語	説明
プロキシサーバ	直接インターネットに接続できない内部ネットワークのコンピュータに代わって、「代理」としてインターネットとの接続を行なうサーバ
ヘッダ	SIP リクエストの概要を示すための情報が含まれる
ボディ	SDP（Session Description Protocol）によって、この後の通話に関する情報を記述する
無線 LAN	無線通信でデータの送受信をする LAN
メディア	音声や映像などの情報
ループバックアドレス	ネットワークカードなどに割り当てられた自分自身を示す IP アドレス

SIP に係る既知の脆弱性に関する調査報告書

－IP ネットワーク上のマルチメディアコミュニケーションシステムのセキュリティ品質向上のために－

［発　　行］２０１０年９月　３０日 第３版
独立行政法人 情報処理推進機構 セキュリティセンター
第３版 執筆、協力
［執　　筆］株式会社ラック
［協　　力］株式会社ネクストジェン

第１版、第２版 執筆、協力
［執　　筆］株式会社ユビテック
株式会社ソフトフロント
［協　　力］エヌ・ティ・ティ・アドバンステクノロジ株式会社（NTT AT）
沖電気工業株式会社
沖電気ネットワークインテグレーション株式会社
株式会社ＯＫＩネットワークス
有限責任中間法人ＪＰＣＥＲＴコーディネーションセンター
日本電気株式会社
日本電信電話株式会社 情報流通プラットフォーム研究所
株式会社 日立製作所
株式会社日立コミュニケーションテクノロジー
富士通株式会社
株式会社富士通研究所

情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。
URL: http://www.ipa.go.jp/security/todoke/

コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

不正アクセス情報

ネットワーク(インターネット、LAN、WAN、パソコン通信など)に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

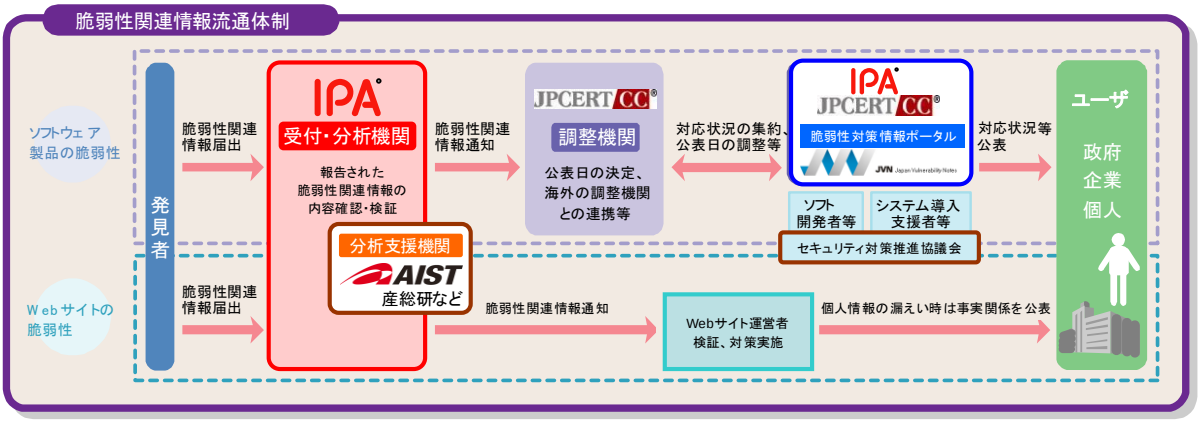
ソフトウエア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウエア、ウェブサーバ等のサーバ上のソフトウエア、プリンタやICカード等のソフトウエアを組み込んだハードウエア等に対する脆弱性を発見した場合に届け出てください。

ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※JPCERT/CC：有限責任中間法人 JPCERT コーディネーション センター、産総研：独立行政法人　産業技術総合研究所

独立行政法人 情報処理推進機構
〒113-6591
東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス16階
http://www.ipa.go.jp

セキュリティセンター
TEL: 03-5978-7527　FAX　03-5978-7518
http://www.ipa.go.jp/security/